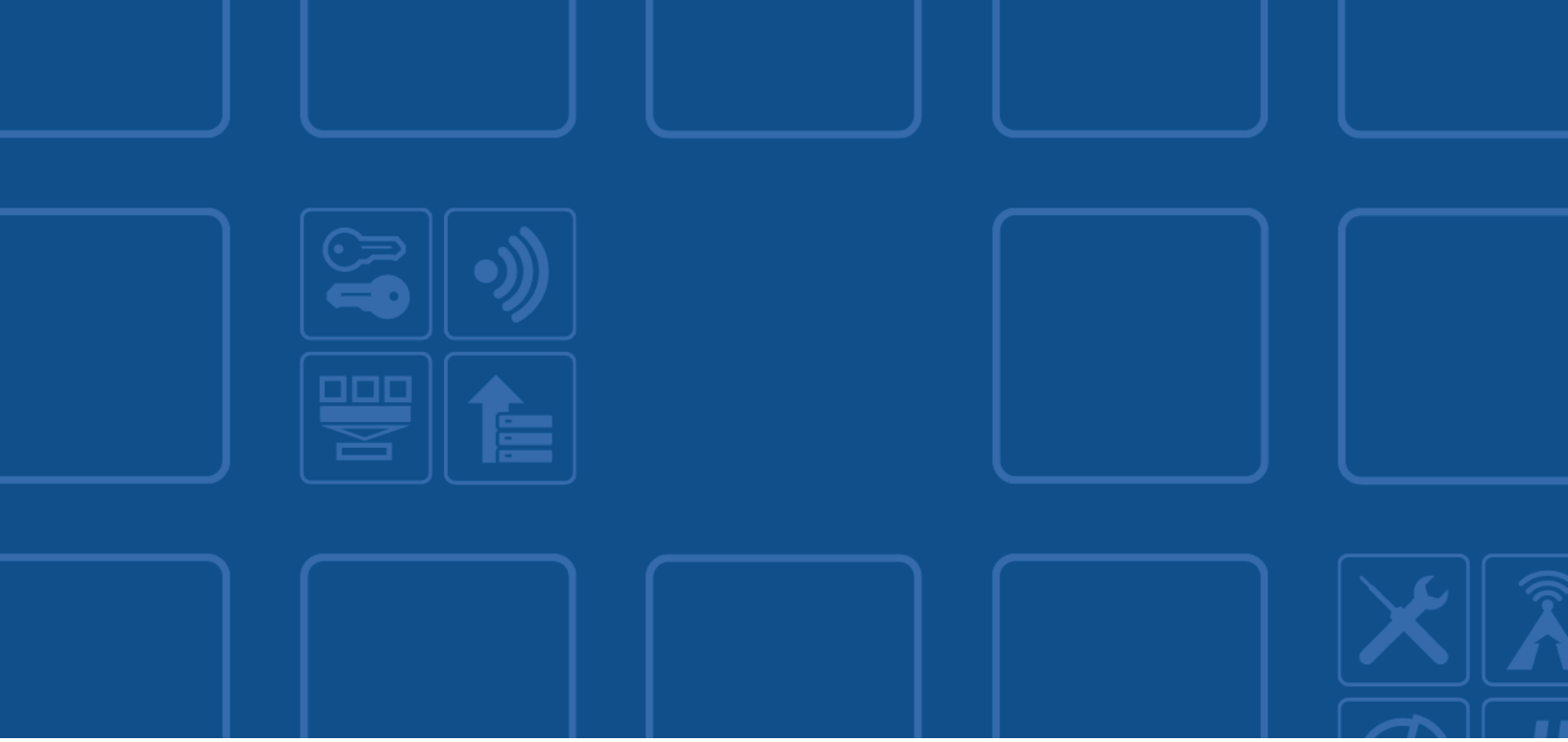
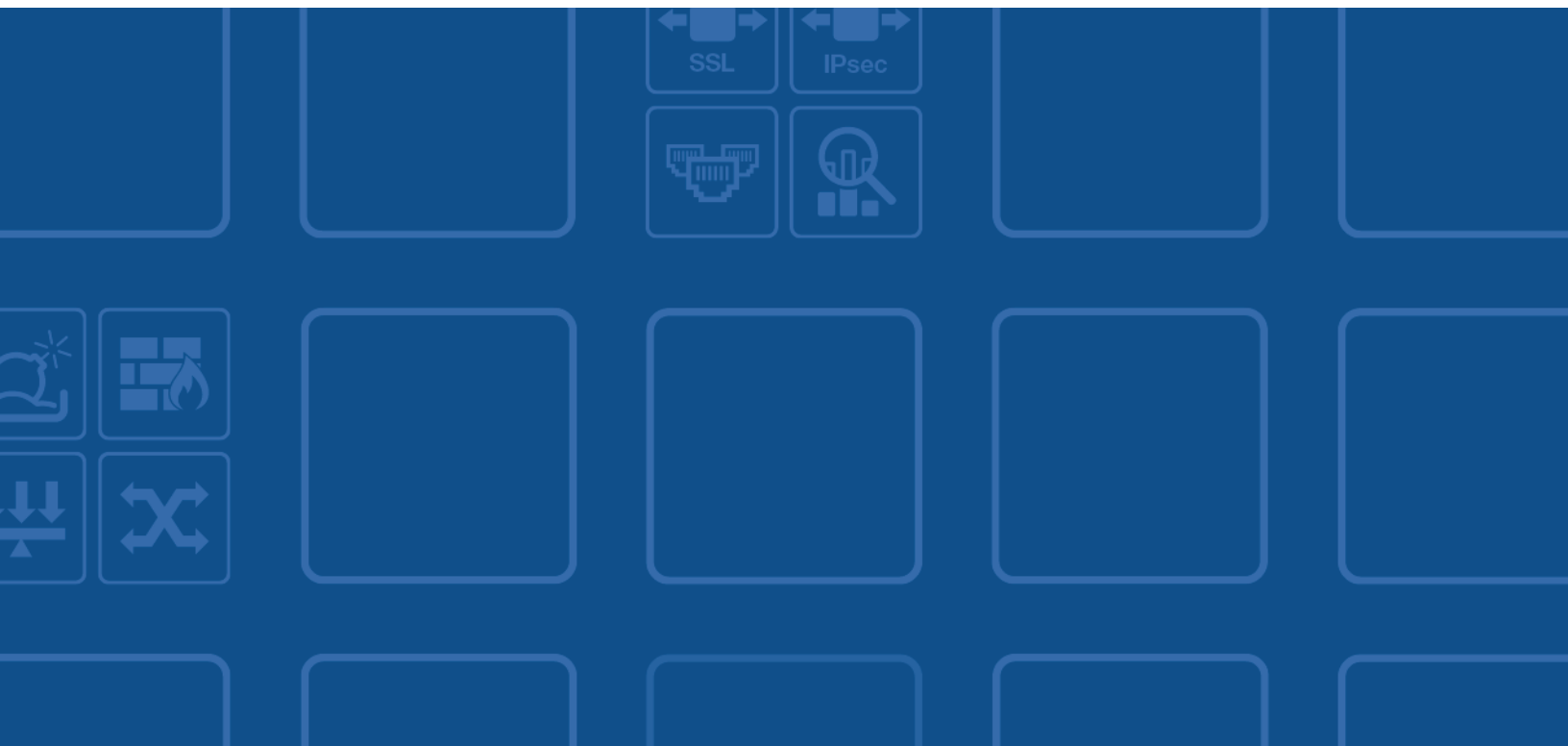


FORTINET
High Performance Network Security

FortiGate Connector for Cisco ACI - Administration Guide

Version 1.2



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Tuesday, June 14, 2016

FortiConnector for Cisco ACI v.1.2 - Administration Guide

01-540-371313-20160505

TABLE OF CONTENTS

Change Log **6**
Overview **7**
Licensing 7
Terms and concepts 8
FortiGate VDOMs 8
FortiOS RESTful API 8
North/South and East/West Traffic 8
Features **9**
Supported Features 9
New to v.1.2 9
Unsupported Features 9
Planned for future releases 10
Supported Fortinet Products **11**
Models 11
Firmware Versions 11
Prerequisites **12**
Cisco Side 12
FortiGate Side 12
Physical Firewall 12
VM Firewall 12
Components of the Device Package **14**
Device model or specification 14
Device script 14
Directory of supporting files 14
Image file or directory 14
Operational modes **15**
Go Through Mode (Layer 2) 15
Go To Mode (Layer 3) 15
Multi-tenant multi-device support 15
Supported use scenarios **16**
Physical Fortigate 16
Go-Through Mode for west-east traffic within data center in ACI 16

Go-To Mode for north-south traffic for Web Server to access DataBase server in data center ... 16
Virtual Fortigate ... 16
Go-Through Mode for west-east traffic within data center in ACI ... 16
Go-To Mode for north-south traffic for Web Server to access DataBase server in data center ... 16
Deployment Procedures ... 17
Device package installation ... 17
Service Deployment ... 17
Importing the Device Package ... 18
Remove Device Package ... 18
Add L4-L7 Device ... 19
GENERAL ... 20
CONNECTIVITY ... 20
CREDENTIALS ... 20
Device 1 ... 20
Cluster ... 21
Create Functional Profile Group ... 21
Remove Functional Profile Group ... 21
Create a Function Profile ... 22
Functional Profile Objects Explanation under “Features”: ... 22
Review ... 25
Service Graph ... 25
Create Service Graph ... 25
Deploy Service Graph ... 26
Modify Service Graph ... 26
Remove Service Graph ... 27
Service Graph deployed ... 29
Installation Variations ... 30
Deploying Data Center Layer 2 Segmentation with Cisco ACI and FortiGate ... 30
Pre-requisites ... 30
Work Flow: ... 30
Create L4-L7 Device with Go-Through mode on Cisco APIC ... 31
Create Functional Profile ... 31
Create Service Graph ... 32
Deploy Service Graph ... 33
Deploying Data Center Layer 3 Segmentation with Cisco ACI and FortiGate ... 35
Introduction: ... 35
Prerequisites: ... 35
Work Flow: ... 36
Configuration: ... 37
Deploying Firewall Service for North-to-South traffic with OSPF ... 51

Introduction: 51
Prerequisites: 51
Work Flow: 51
Configuration: 52
Deploying Firewall service with Fortigate-VM and VmWare 67
Pre-requisite 67
Work Flow: 67
Configuration 67
Deploy the firewall device shared by multiple service graphs 72
Pre-requisite 72
Work Flow: 72
Configuration 72
Deploying High Availability Service with Cisco ACI and FortiGate 83
Pre-requisite 83
Work Flow: 83
APIC Infrastructure and FortiGate rollback 85
Basic Troubleshooting 86
Verify Service Graph deployed 86
Service deployed but parameters missing 87

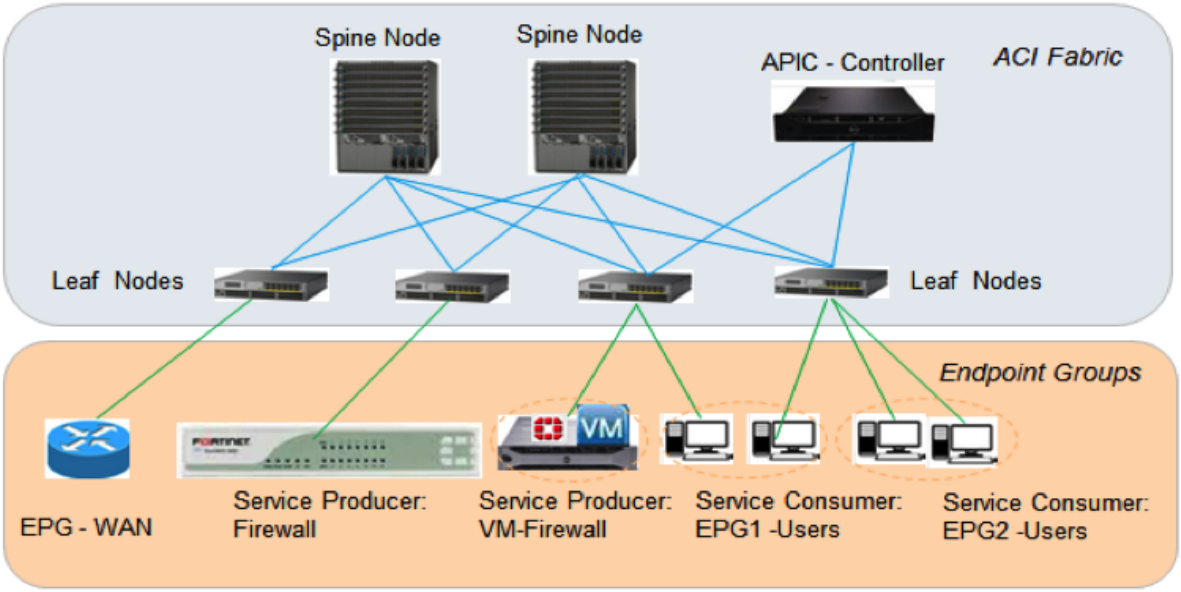
Change Log

Date	Change Description
2016-05-09	Initial Release of version 1.2
2016-06-14	Deploying High Availability Service with Cisco ACI and FortiGate

Overview

FortiGate Connector for Cisco ACI (Application Centric Infrastructure) is the Fortinet solution to provide seamless integration between Fortinet Firewall (Fortigate) deployments and the Cisco APIC (Application Policy Infrastructure Controller). This integration allows customers to perform single point of FortiGate configuration and Management operation through Cisco APIC.

While the FortiGate series of firewalls enable superb firewall services, in a data center environment, the insertion, configuration, and management of network services such as firewall can be quite complex and potentially error-prone tasks. One solution for such data center problems is Cisco's ACI. Cisco's ACI is a policy-based framework with integration of software and hardware in the underlying leaf-spine fabric. In Cisco ACI, the APIC is a tool used to automate service insertion and provisioning into the fabric of the network environment. Network service appliances, both physical and virtual, can be attached to ACI fabric's leaf node through APIC. Traffic demanding certain network services is steered by APIC-managed policies to the appropriate resources. The FortiGate Connector allows FortiGates to be included amongst the list of resources that traffic can be directed to.



Licensing

FortiGate Connector for Cisco ACI is free of charge for Fortinet customers. You need to make sure that you register your FortiGate with FortiCare on support.fortinet.com.

Terms and concepts

FortiGate VDOMs

VDOM or Virtual Domain refers to a discretely administered segment on a FortiGate firewall. A FortiGate firewall that is not segmented and where a single administrator can access all of the firewall is operating in the “root” VDOM. However, it is possible to segment the FortiGate so that different administrators can access different areas of the FortiGate. Credentials for VDOM X will allow access to the resources and settings of VDOM A but no other. There will also be global resources and settings that will require credentials to the root VDOM. When setting up connectivity between Cisco APIC and the FortiGates it will be important to know which VDOMs control the needed resources.

FortiOS RESTful API

REST (sometimes spelled ReST) stands for Representational State Transfer. It is a software architectural style for the WWW. REST systems typically communication over HTTP, using HTTP verbs or commands to retrieve and send information to remote servers.

A good resource for the finer details of Fortinet’s implementation of ReST can be found at http://docs.fortinet.com/uploaded/files/1276/FortiAuthenticator_REST_API_Solution_Guide.pdf

North/South and East/West Traffic

The cardinal compass direction terms to describe traffic flow are used to differentiate between traffic within the cloud or data center and traffic going in and out of the cloud or data center.

- North/South - traffic either heading into or out of a cloud or data center.
- East/West - traffic that is between nodes inside the same cloud or data center.

Features

There are a number of features associated with firewalls in general and FortiGate firewalls in particular. This section should explain which of these features are available through the FortiGate Connector and which are not.

Supported Features

The FortiGate Connector for Cisco ACI supports the following functions:

- Cisco ACI service insertion - software package for FortiGate device deployed to Cisco APIC, containing FortiGate models, function description, version, credentials, as a L4-L7 service.
- Enable tenant configuration to add/modify/delete L4-L7 device of FortiGate firewall service.
- Enable FortiGate deployment as both physical and virtual device (FortiGate chassis & VM).
- Support both transparent (GoThrough) and L3 (GoTo) device mode .
- Automatically create VDOM (context). One VDOM per logical device under a tenant.
- Enable FortiGate specific interface configuration: physical interface and port channel.
- Support IP address configuration on Layer 3 interfaces.
- Support subnet, service and schedule object configuration.
- Enable FortiGate firewall device to connect to endpoint groups (EPGs).
- Support IPv4 policies: match, action, network operations & security features selection (although the Enable/Disable Security profile option in policies is not supported).
- Support NAT.
- Enable service graph to add/modify/delete FortiGate firewall service node.

New to v.1.2

The Fortigate Connector v1.2 for Cisco ACI has added support for the following functions:

- High Availability (Active-Standby Mode)
- OSPF based routing configuration in the L3 (GoTo) mode
- Support for logging and error reporting of Fortigate as a L4-L7 device
- Automatically create VDOM based on APIC virtual device ID
- Policy enable/disable support
- Enable/Disable DDoS features
- Enable/Disable UTM Security Profiles

Unsupported Features

The following features normally found on FortiGates are not supported through the FortiGate Connector for Cisco ACI.

- Proxy Policy
- SSL/SSH Inspection
- FortiGate WAN load balance link.
- Administrator profile for limited access of different administrator accounts.
- Firewall port forwarding (destination NAT).
- Firewall logging: allowed traffic, security events, all sessions, etc.
- Firewall packet capture.
- Firewall with FortiGuard DDNS.
- Other Firewall features not specifically listed as supported.

The following information resources are available on the FortiGates but do not integrate with APIC:

- Error Logs
- Statistics Reporting

The unsupported features on APIC may still be used on FortiGate outside of the APIC control; the user must login to FortiGate to configure, monitor, and debug. However, any conflict with the operations from APIC may cause malfunction.

Planned for future releases

FortiGate Connector for Cisco ACI plans to incorporate the following features and functions into future versions of the software:

- Support for BGP-based routing configuration in the L3 (GoTo) mode from APIC.
- Monitor FortiGate devices (health) status.
- Provide FortiGate device statistics – device and service counters per context.
- Support D-NAT configurations
- Support IPv6 policy configurations
- Performance reporting: control and management plane based on APIC, data path on FortiGate.
- Support of Dynamic EPG

New features are not limited to this list. These are just the features currently planned for.

Supported Fortinet Products

The supported Fortinet products refers to those that are compatible with the FortiGate Connector for Cisco ACI software, and will properly integrate into the Cisco ACI. The products are separated into models and firmware but it is an “and” set of parameters. In order to be supported the Fortinet product has to be one of the listed models running supported firmware.

Models

FortiGate Connector for Cisco ACI v1.1.x and 1.2.x support integration with the following predefined models:

- FG-600D
- FG-900D
- FG-1000D
- FG-1200D
- FG-1500D
- FG-3000D
- FG-3100D
- FG-3200D
- FG-3700D
- FG-VM
- Unknown (to be added based on customer's request)

Firmware Versions

FortiGate Connector v1.2 for Cisco ACI is compatible with the following FortiOS firmware:

- FortiOS 5.4 and above

Prerequisites

Cisco Side

Before the FortiGate Connector for Cisco ACI can be successfully deployed, a number of prerequisites need to be satisfied within the Cisco environment.

One of the following Cisco ACI environments needs to be in place:

- Cisco ACI v1.2(2.g) or later

Within the Cisco ACI, the following configurations need to be completed before Layer 4 -7 Services (in this case, the FortiGate Connector) can be deployed:

- Creation of Access Policies configuration under Fabric menu
- Creation of any need Tenant(s)
- Creation of Network(s) (including Bridge Domain)
- Creation of Application Profile(s)
- Creation of End Point Group(s)
- Creation of Contract(s)
- Create OSPF L3Out (Only if OSPF is required)

For detail, please consult Cisco APIC deployment Guide.

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/L4-L7_Services_Deployment/guide/b_L4L7_Deploy.html

FortiGate Side

Before the FortiGate Connector for Cisco ACI can be successfully deployed, a number of prerequisites need to be satisfied on the FortiGate side of the equation.

Physical Firewall

1. Configure administrator user name and password.
2. Enable http/https on mgmt. port.
3. Configure IP address in mgmt. port.
4. Enable VDOM-Admin globally.
5. Configure Port-Group if needed.

VM Firewall

1. Assign network ports before start VM
2. Configure administrator user name and password.
3. Enable http/https on mgmt. port.

4. Configure IP address in mgmt. Ports
5. Enable VDOM-Admin globally

Components of the Device Package

To add a network service to ACI fabric, the service's device package needs to be uploaded to APIC. The device package is a zip file containing these components:

Device model or specification

The Device Specification is an XML file called `DeviceModel.xml` that covers descriptions of FortiGate devices, interfaces, connectivity and services. The file contains a hierarchical description of FortiGate devices, including:

- Device functions
- Parameters of each function
- Interfaces/network connectivity information of each function.

Device script

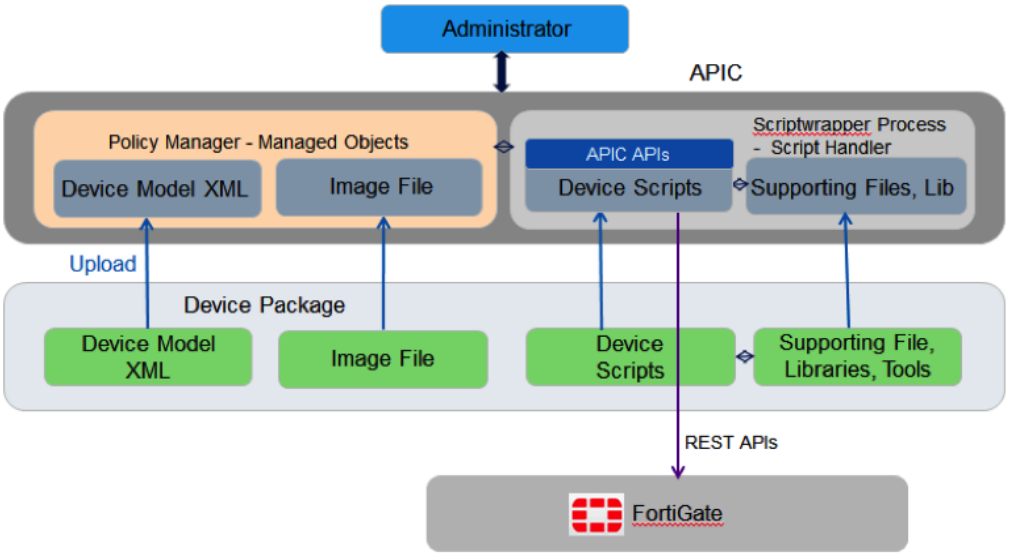
This is a Python file, `DeviceScript.py` with API functions to interface between the Cisco APIC and the FortiGate REST APIs. This Python file is associated by the DeviceModel.xml device specification to device script for APIC.

Directory of supporting files

This component contains supporting Python files, text files and libraries of scripts and tools.

Image file or directory

The directory contains file(s) such as a Fortinet icon (`Fortinet_name.gif`) to be displayed on the APIC management page.



Operational modes

There are two types of network service devices which Cisco APIC integrates with. These types of devices are defined by their operation mode. They are either Go Through or Go To. Normally a device has to be preconfigured as one of these types before its imported package is managed by the APIC.

Go Through Mode (Layer 2)

Devices in Go Through mode are considered layer 2 devices (from the OSI model) and are sometimes known as transparent. They are referred to as transparent because while the traffic goes through them and can be affected by them, they are not seen by the network and are not a destination in their own right for the traffic. They do not route traffic. These devices are not referred to by the packet's destination MAC or IP address. In most cases, these devices will only have an address for the purposes of management.

Go To Mode (Layer 3)

Devices in Go To mode are considered Layer 3 (from the OSI model) devices. They can route traffic and they are referenced as the destination in a packet's destination MAC address or destination IP address.

Multi-tenant multi-device support

- Multi-tenant Multi-device is typical in the use cases of this project. The support is worth more detailed description. When FortiGate device is added a tenant's L4-L7 services, multi-context aware can be enabled. This indicates to the device package that the L4-L7 device is going to be a virtual device that shares resources with other tenants on the FortiGate. In FortiGate implementation, this virtual device is represented by a VDOM. Under each tenant, multiple such virtual devices can be configured. VDOM name is the virtual device ID generated by APIC when a virtual device is added.
- Each tenant sees all available interfaces and can share interfaces (ports) with other tenants, if it is multi-context aware. For Physical Device under L3 Routed (GoTo) Mode, Tenant can share physical interface as VLAN is used to isolate the physical interface. In VM Device, this is not true. You can only use dedicated VNIC.

Supported use scenarios

Physical Fortigate

Go-Through Mode for west-east traffic within data center in ACI.

Scenario: Web server and back-end database servers have same subnet in data center; customer needs firewall service between web server and back-end database servers.

Go-To Mode for north-south traffic for Web Server to access DataBase server in data center.

Scenario: Firewall service for Web Server to access DataBase server in data center.

Virtual Fortigate

Go-Through Mode for west-east traffic within data center in ACI.

Scenario: Web server and back-end database servers have same subnet in data center; customer needs firewall service between web server and back-end database servers.

Go-To Mode for north-south traffic for Web Server to access DataBase server in data center.

Scenario: Firewall service for Web Server to access DataBase server in data center.

Deployment Procedures

Below sections, we will walk through the high level of how to deploy a service insertion as well as detail procedures of how to perform each steps.

Device package installation

To successfully deploy Fortigate Connector into Cisco APIC, customers need to perform the following steps:

1. Import Device Package
2. Add L4-L7 Device
3. Create Functional Profile
4. Create Service Graph Template
5. Deploy Service Graph Template.

Service Deployment

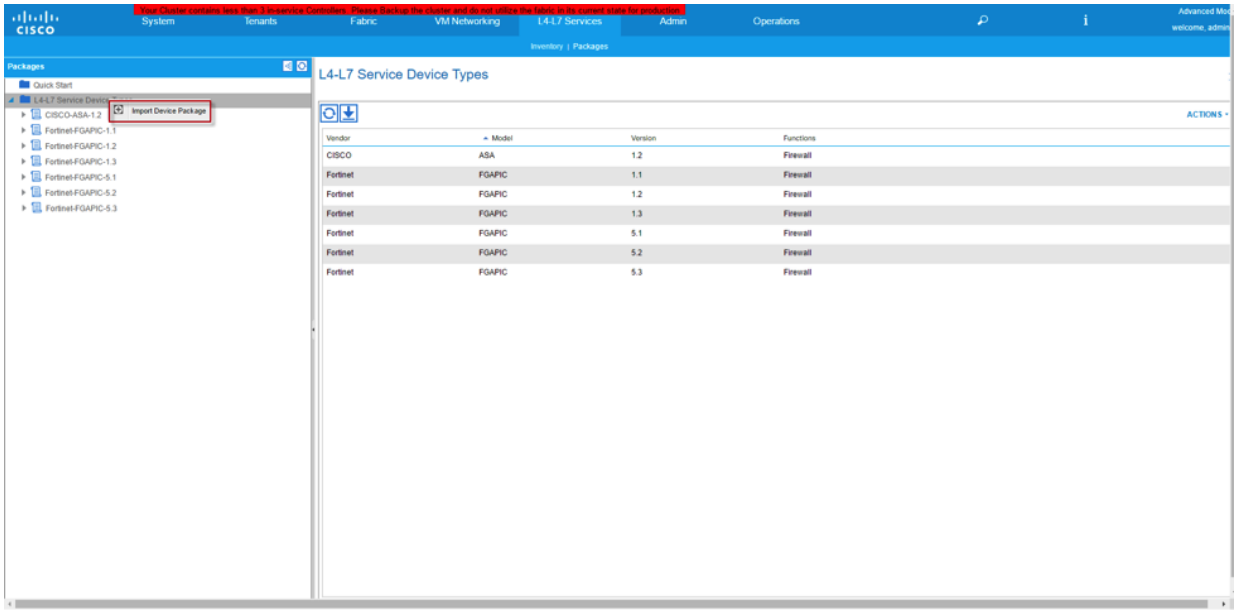
According to the APIC deployment guide, a service device introduces a Layer 4 to Layer 7 service by this typical procedure:

1. Import the device package of the service device,
2. Configure a tenant who asks for network services,
3. Register the device and its logical interfaces,
4. Configure logical device parameters,
5. Configure a layer 3 network,
6. Configure a bridge domain,
7. Configure an application profile,
8. Configure a physical domain (or VMM domain),
9. Configure a VLAN pool,
10. Configure a contract
11. Configure a management endpoint group (EPG),
12. Configure a service graph template,
13. Select default service graph template parameters,
14. Attach the service graph template to a contract
15. Configure additional configuration parameters.

To add a support of a non-Cisco firewall device in the Cisco ACI fabric based data center, a device package should be developed for the APIC. Then the remaining task is standard APIC deployment of a network service device.

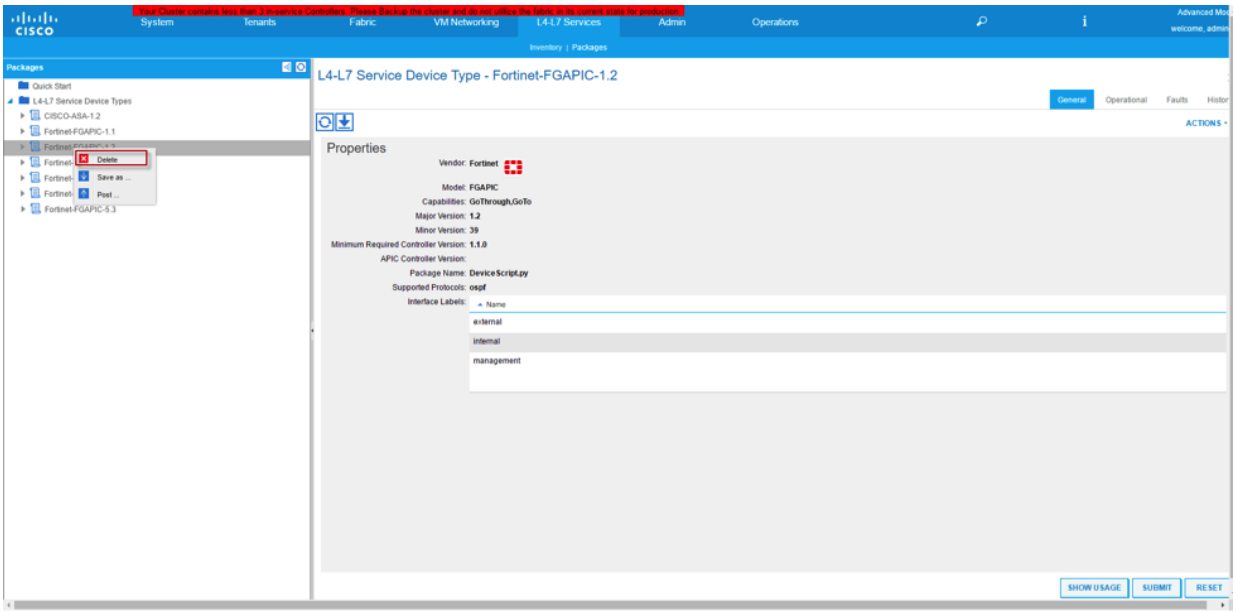
Importing the Device Package

1. Download Device Connector Package from Fortinet Support Web (URL) site to local storage.
2. From APIC menu, Navigate to ***L4-L7 Services > Packages*** and right click on ***L4-L7 Device Type*** on the left hand panel. Select ***Import Device Package***



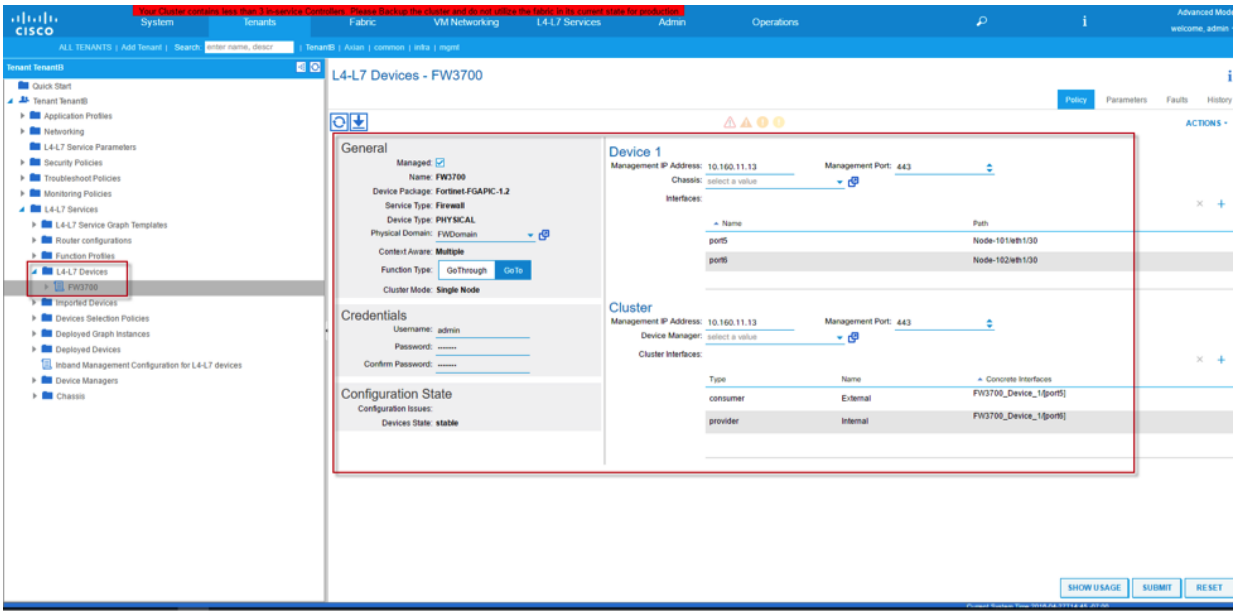
Remove Device Package

To remove Device Package, navigate to ***L4-L7 Services > Packages*** and right click on the Device package on the left panel and select ***Delete*** option.



Add L4-L7 Device

Within Tenant, Expand ***L4-L7 Services > L4-L7 Devices***, right click on mouse and select "***Create L4-L7 devices***"



GENERAL

Field	Description / Options
Name	Name of the Device
Device Package	Select Device Package from drop down list
Model	<List of the supported models>
Mode	• Single Node / HA Cluster
Function Type	• GoThrough (L2) • Goto (L3)

CONNECTIVITY

Field	Description / Options
Physical Domain or VMM Domain	Select from drop down list Domain which you should have configured during APIC Access Policies setup
APIC to Device	• Out-of-Band • In-Band

CREDENTIALS

Field	Description
Username	<login name to the Fortigate>
Password	<Password to login to Fortigate>
Confirm Password	<Password to login to Fortigate>

Device 1

Field	Description / Options
Management IP Address	<IP address to connect to Fortigate>

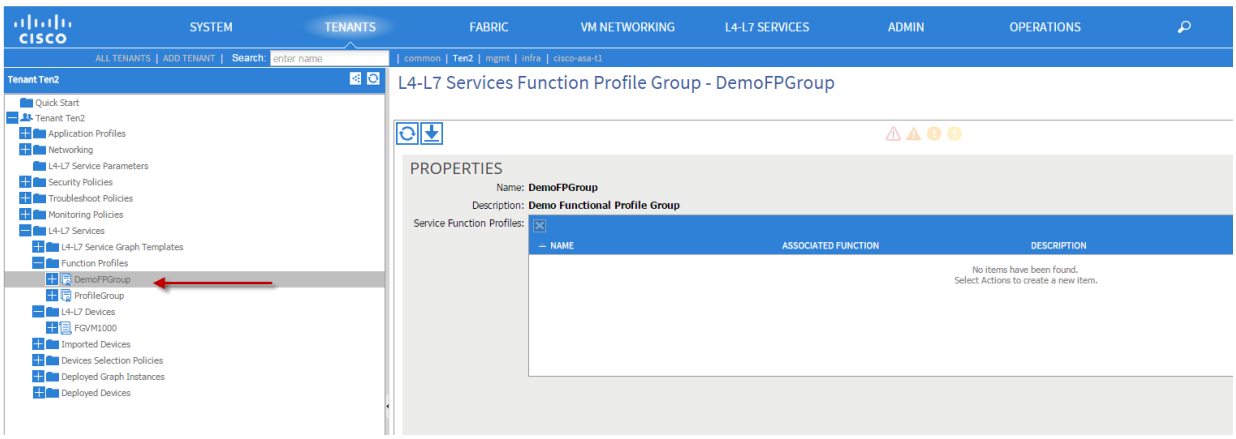
Field	Description / Options
Management Port	• http • https https is the prefer method
Connects To	• Port (Default), PC, VPC
Physical Interfaces	Click on "+" sign to add interfaces connecting from APIC to FortiGate
Name	Select from Drop down list to select port. (If using Port Channel, please type in the correct Port Channel name ex:PO1, PO2..etc.)

Cluster

Configure all the fields same as Device 1, with exception to Cluster Interface.

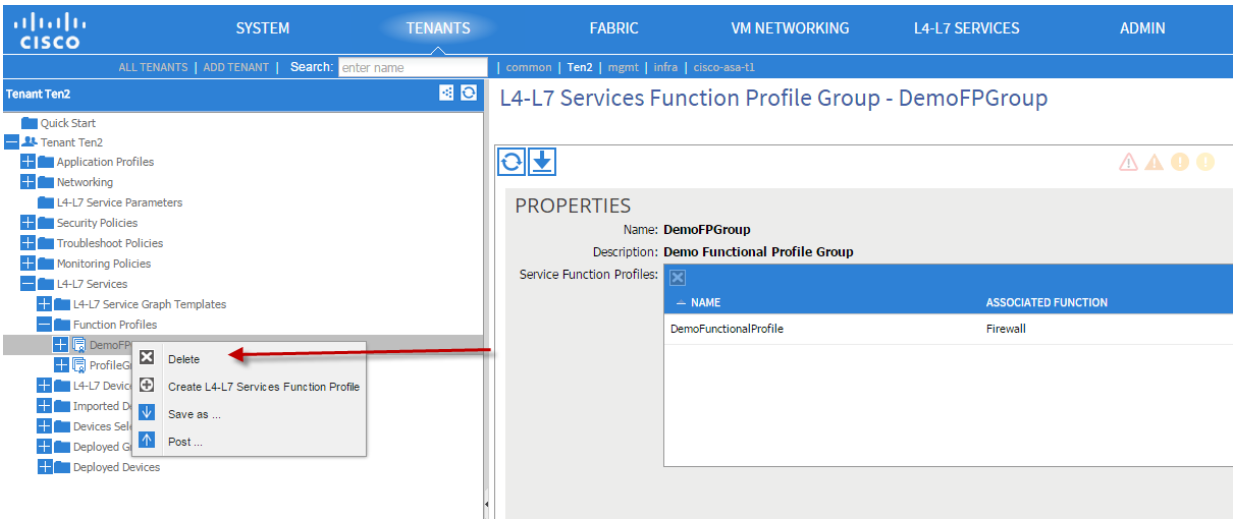
For Cluster Interface, click the "+" icon to add logical device interfaces.

Create Functional Profile Group



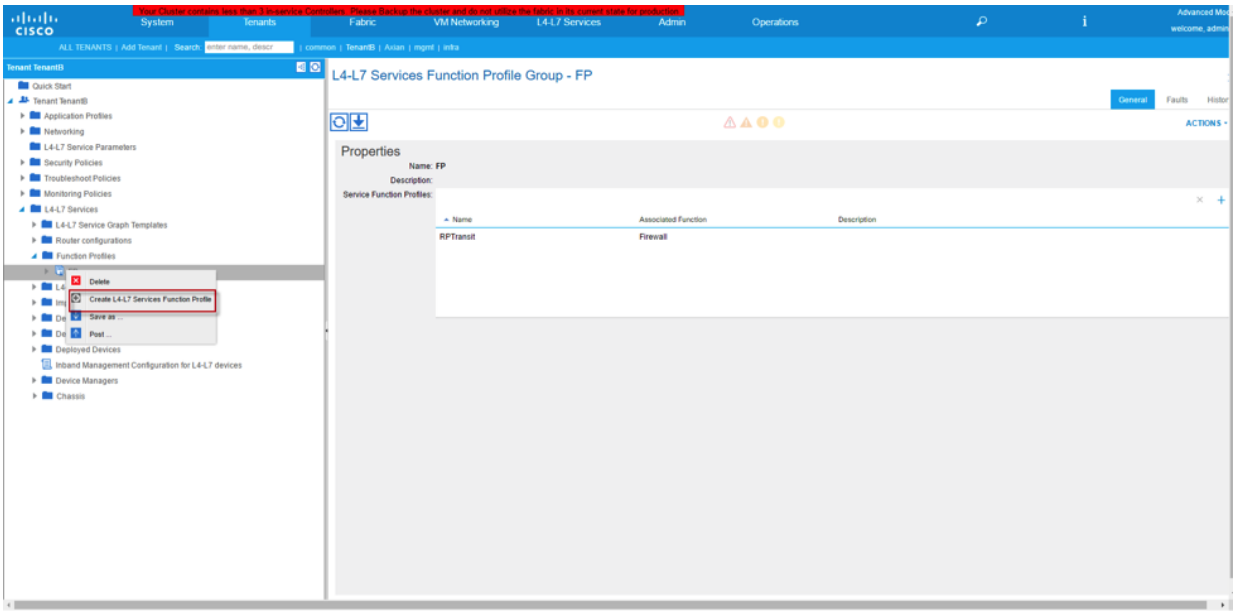
Remove Functional Profile Group

To remove Functional Profile Group, navigate to ***Tenant > L4-L7 Services > Functional Profiles*** and right click on the Functional Profile group name listed on the left hand panel and select ***Delete*** option.



Create a Function Profile

Functional Profile defines the template for the Service(s) that is going to deploy such as L4-L7 Device Interface IP addresses, Rule ID, Object Addresses, Policy Rules, Source/Destination Ports…etc.



Functional Profile Objects Explanation under “Features”:

Device Network:

Contained External and Internal Interfaces that will be programmed onto Fortigate VDOM. This is the interfaces (typically external and internal) that will be associated to the VDOM. If user intends to have multiple legs deployment scenario, this is where he/she can add additional interfaces with unique name.

Beginning with FortiGate Connector v1.2, the device package no longer has the option to select VDOM mode and VDOM name. Instead, the VDOM name is automatically generated based on virtual device ID from APIC; the VDOM mode is based selection of Go-to mode and Go-through mode during the device creation. If Go-to mode is selected, user must input IP addresses and subnet mask for each interface; if Go-through mode is selected, user must leave IP address field untouched.

Firewall Objects:

This field allows user to customize Firewall Addresses, Service and scheduling.

Firewall Policy Rule:

This field encompassed the creation of Firewall policy that will be program onto FortiGate. Security Profile and Logging Options can be enabled or disabled here.

If user intends to use multiple service graphs shared by same virtual device, please ensure the rule ID, policy names are all unique across all service graphs. Otherwise, policy rules will overwrite each other.

We made changes on this release to allow better policy sorting function. The “Name” Column under FireWallPolicyRuleID (Figure 1) will only take numeric entry. This field is equivalent to “Policy ID” on the Fortigate. We have added additional sub-fields under this folder and they are “Name” and “OrderNo” respectively (Figure 2). The “Name” sub-field is equivalent to “Policy Rule Name” on the Fortigate and this field is optional. The “OrderNo” sub-field is a mandatory field where we leverage it to sort the ordering of the policy. The lower policy number will be listed first on the Fortigate. In the case of share VDOM with multiple service graphs, the rule above applied where the RuleID and policy names need to be unique.

Figure 1

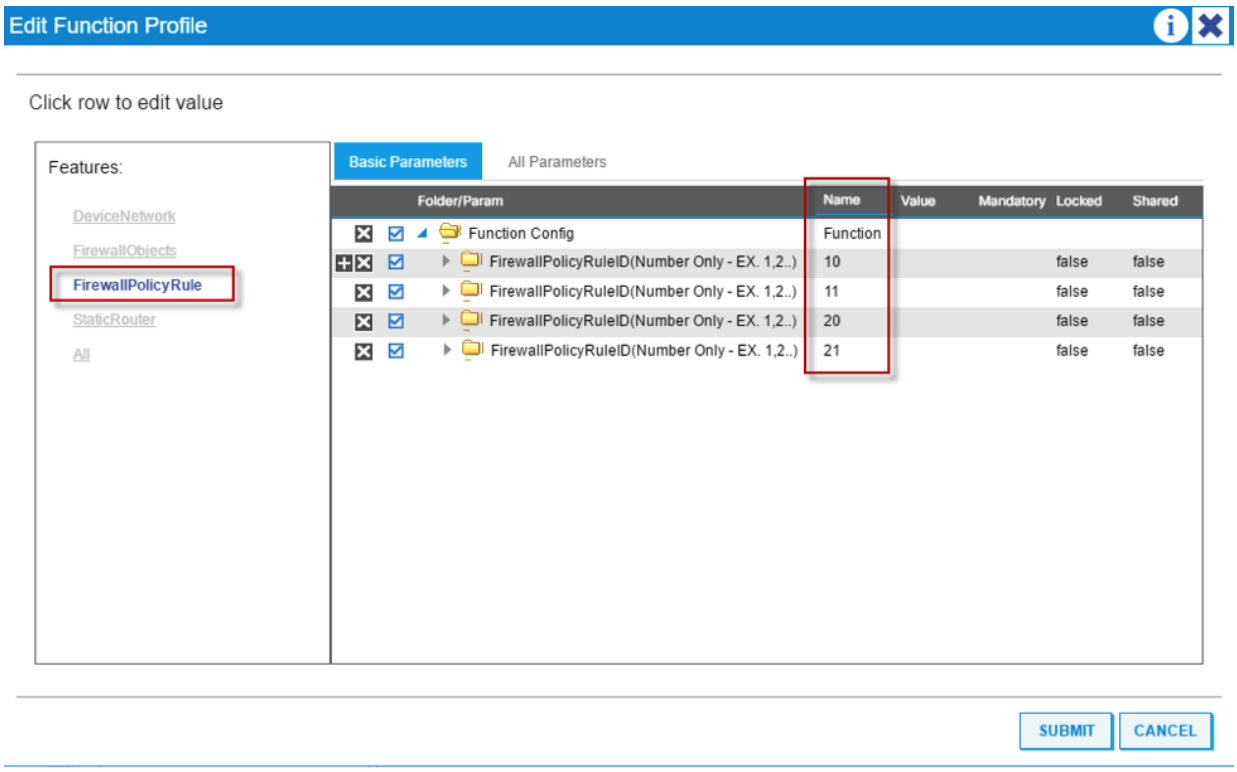
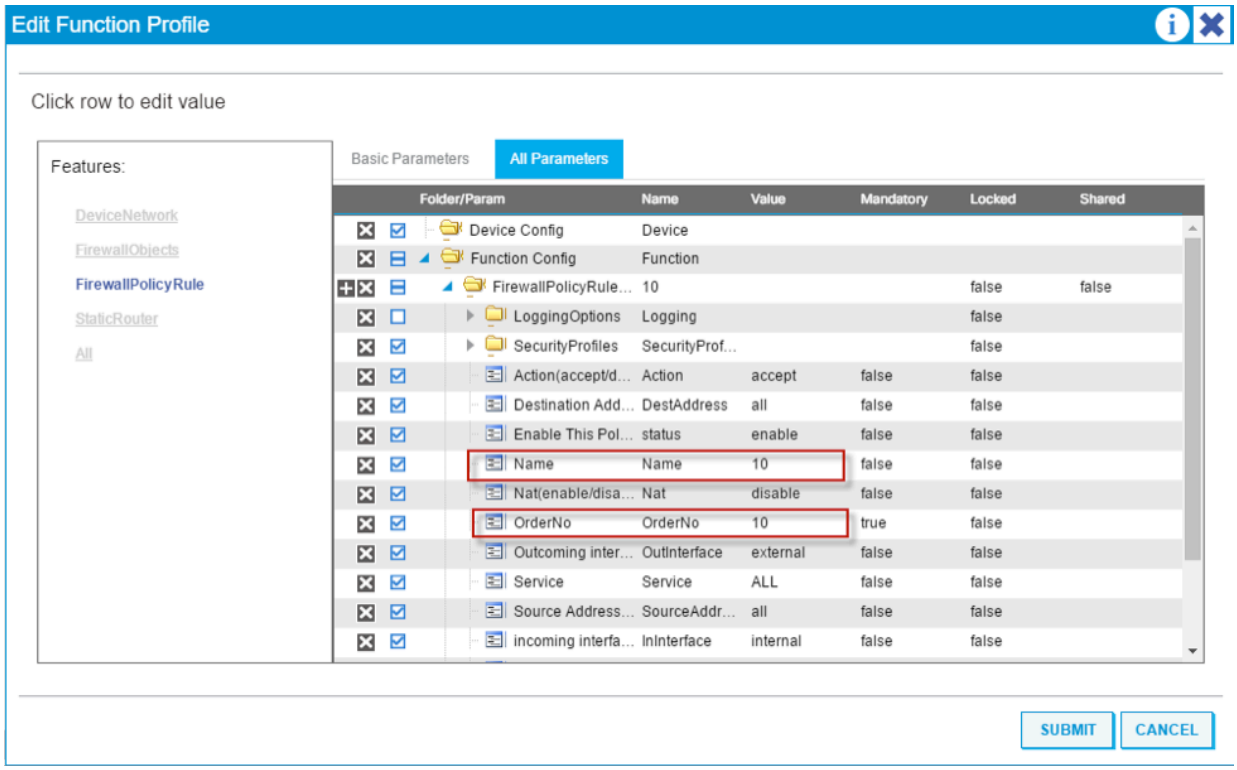


Figure 2



Static Router:

Allow user to configure static route that will be used on Fortigate.

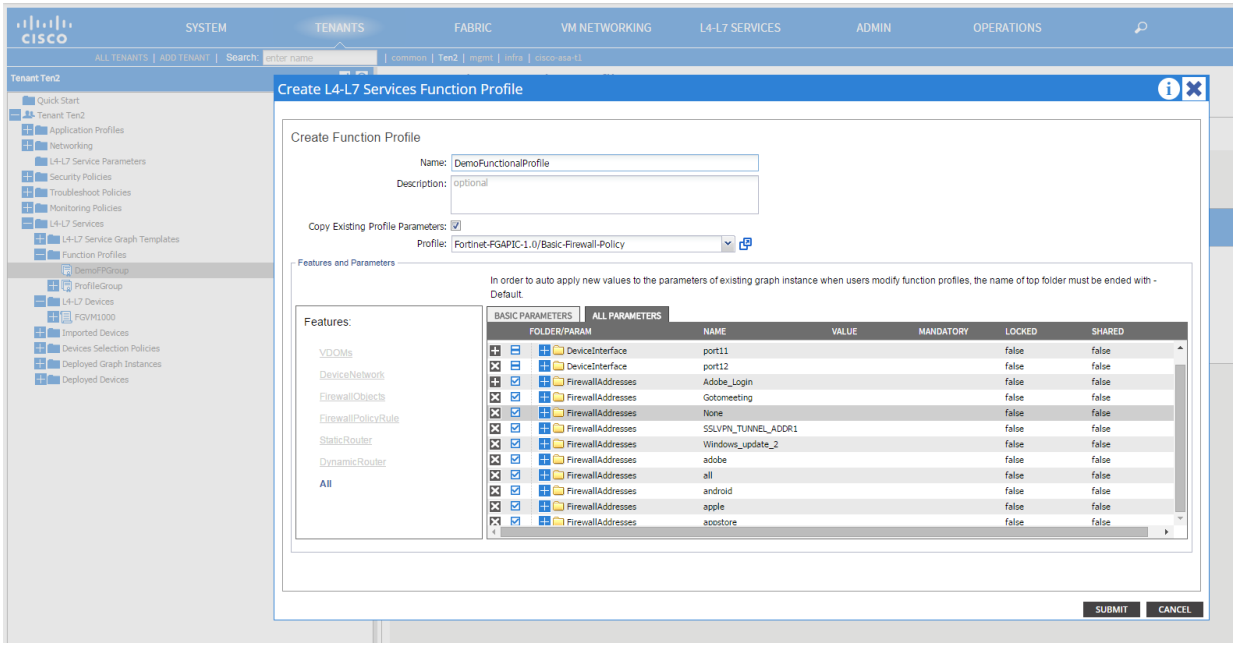
All:

This field listed all the parameters stated above plus DDOS configuration.

If user is using multiple legs shared by same virtual device, please ensure to select appropriate interface names created earlier from Device Network field

Review

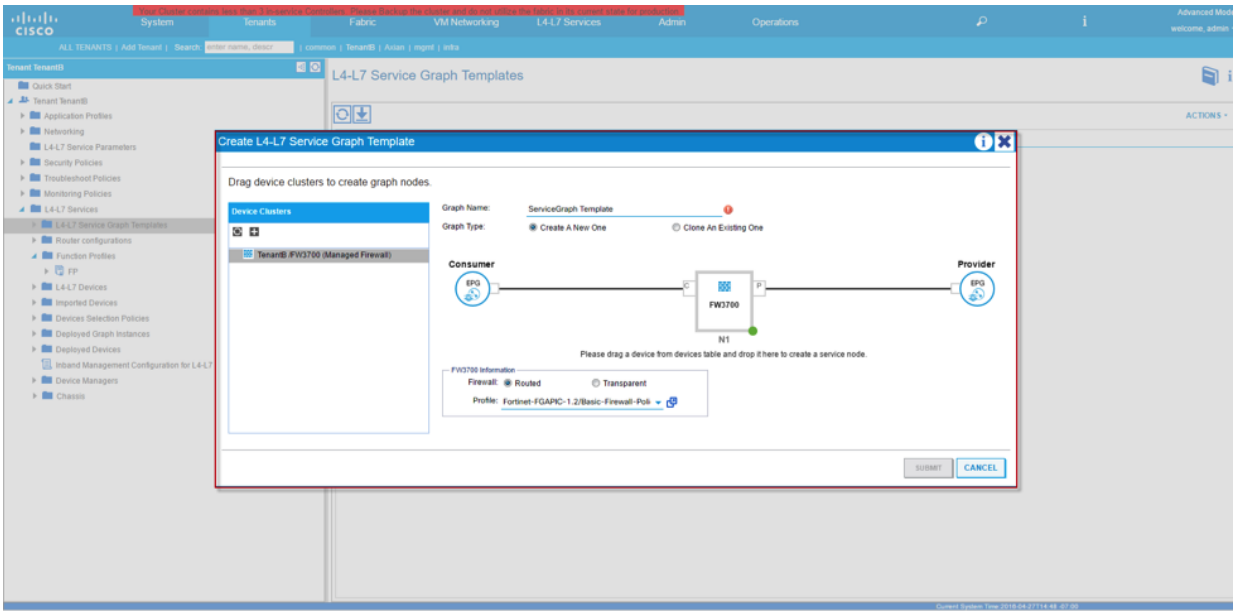
All Field display all the fields in the features listing. If you are satisfy with all your inputs, then hit the submit button to complete your creation of Functional Profile template.



Service Graph

Create Service Graph

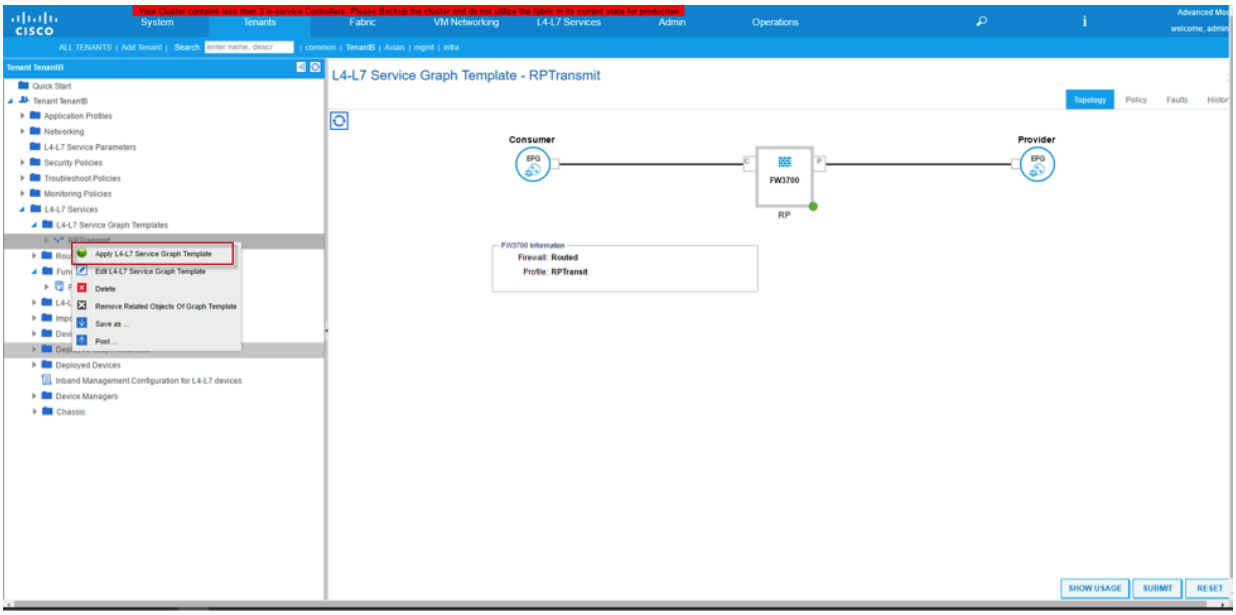
Service Graph template is used to tightly coupled the Functional Profile or Firewall configuration and combine with the Firewall device we defined at earlier steps.



Right Click on ***L4-L7 Service Graph Template*** to create a Service Graph.

Deploy Service Graph

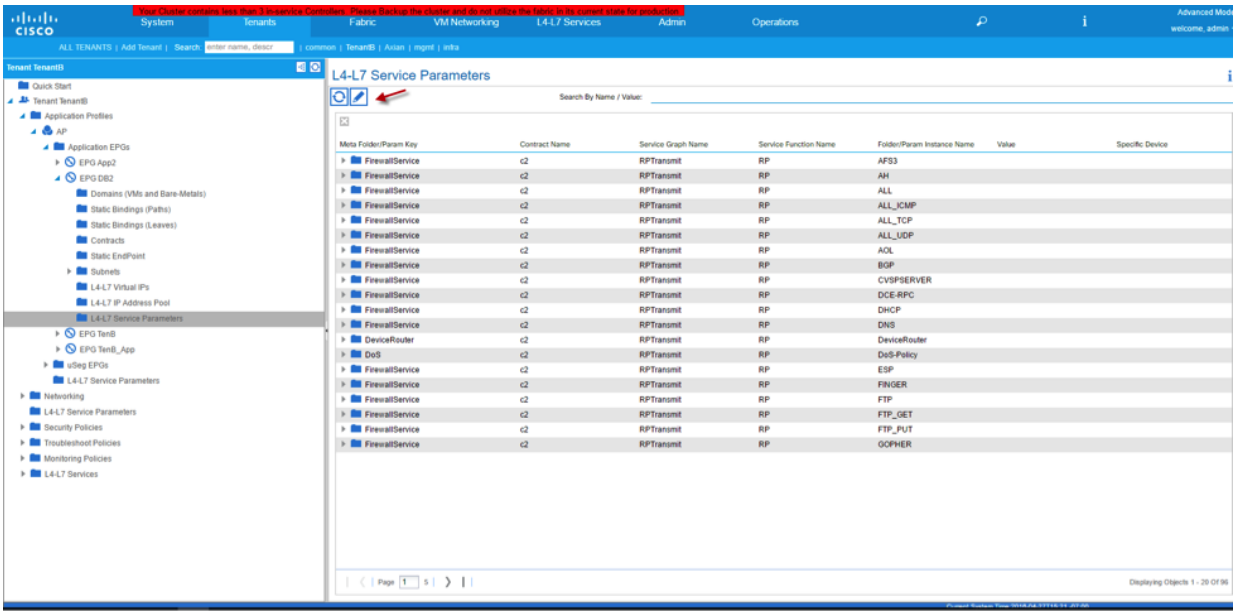
Once we combined the Firewall configuration and associated device together, we are ready to deploy the service Graph to create a VDOM automatically.



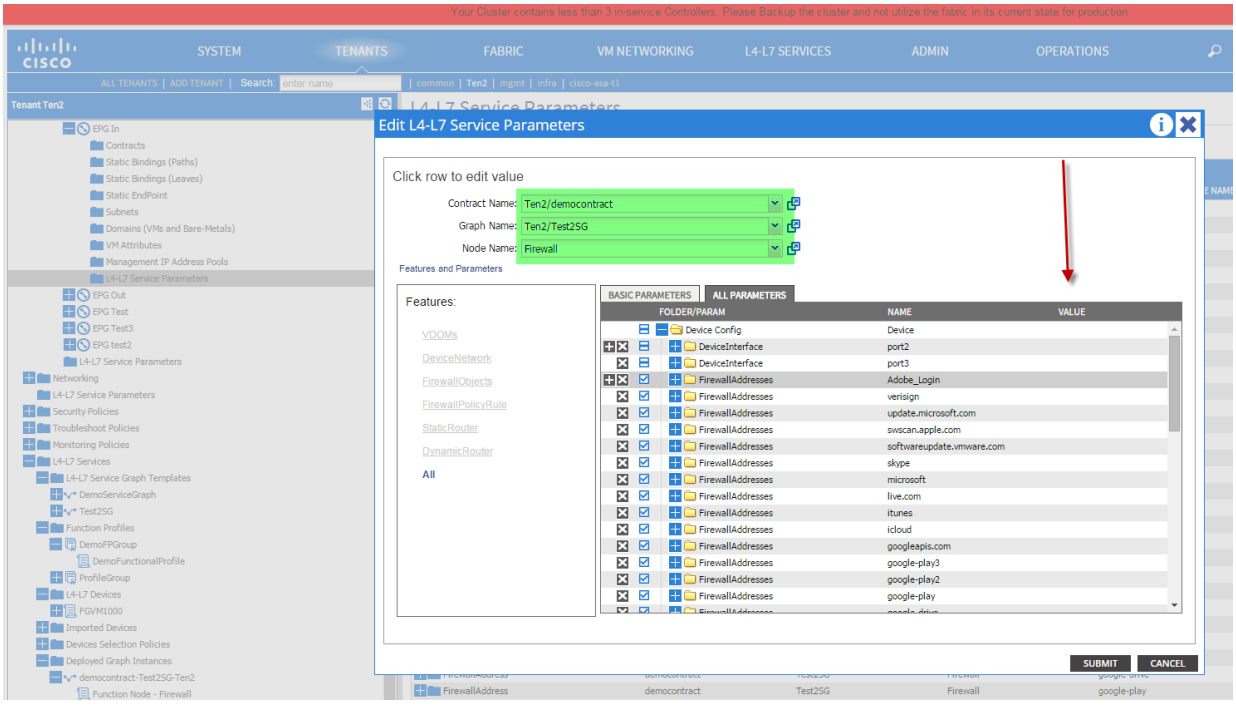
1. Right Click on Service Graph defined from above and select ***Apply L4-L7 Service Graph Template.***

Modify Service Graph

1. Navigate to ***Tenant>Provider EPG>L4-L7 Service Parameters*** and select the pen icon, which will lead you into edit mode to modify parameters on deployed Service Graph.

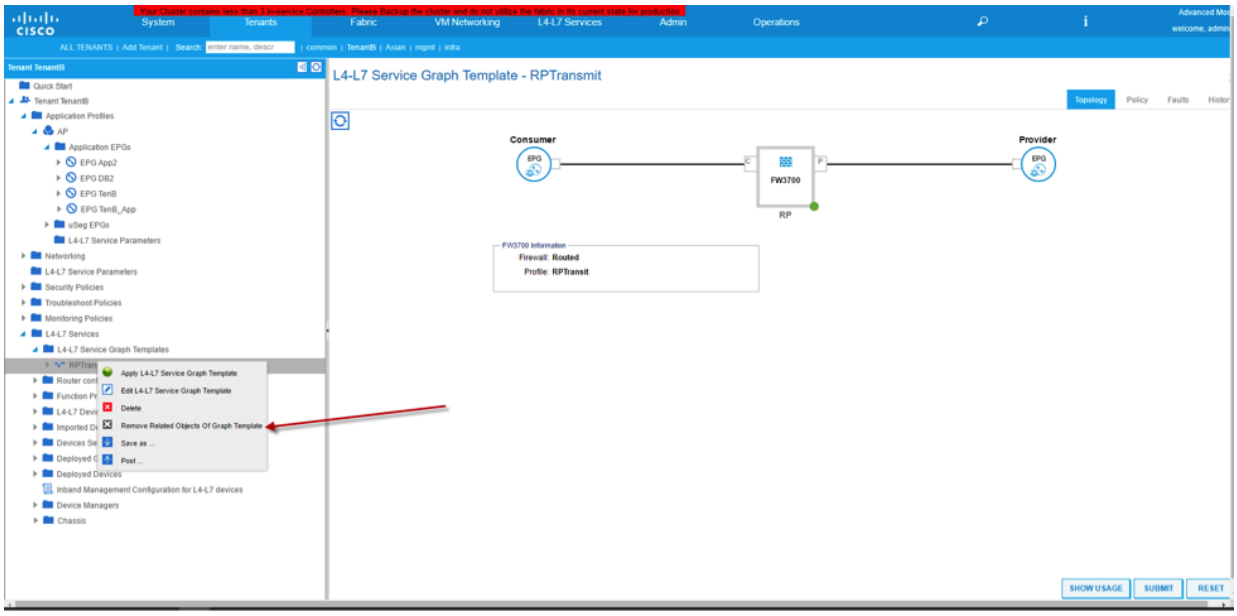


2. On the next screen, select the Contract name, Graph Name and Node name from the drop down list and all the associated Service Graph Parameters will be displayed.
3. Expand the field you want to make modification and change the appropriate value from the drop down list and then hit submit.



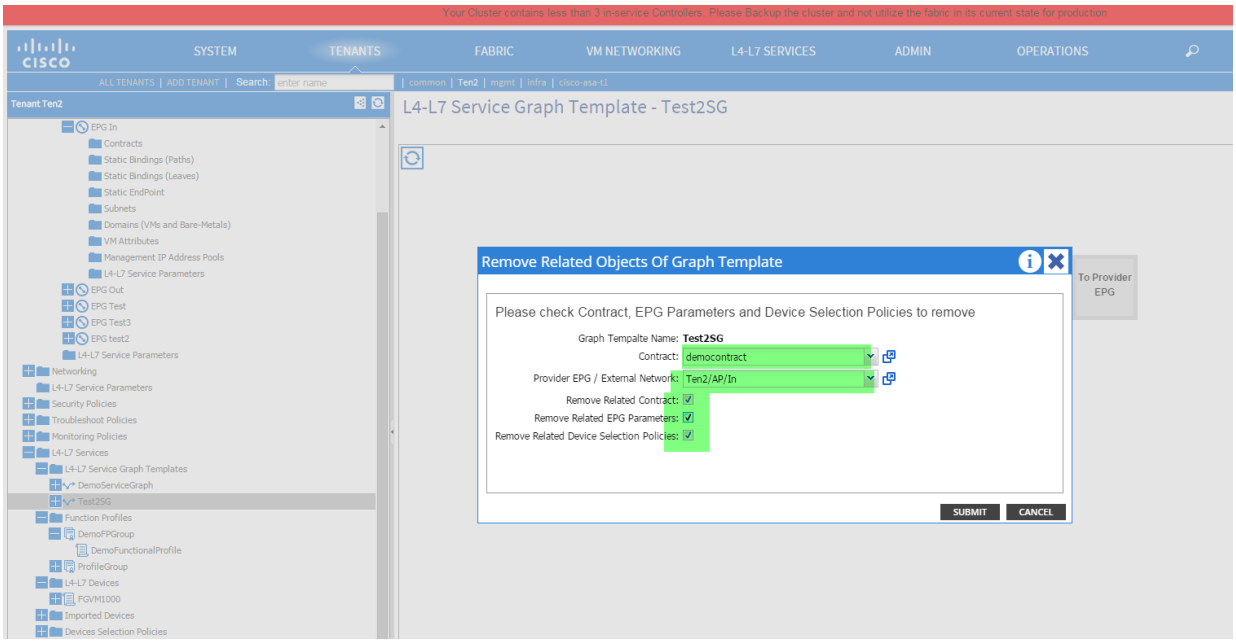
Remove Service Graph

1. Navigate to ***Tenant>L4-L7 Services>L4-L7 Service Graph Templates***. Right click on Service Graph template and select***Remove Related Objects Of Graph Template.***



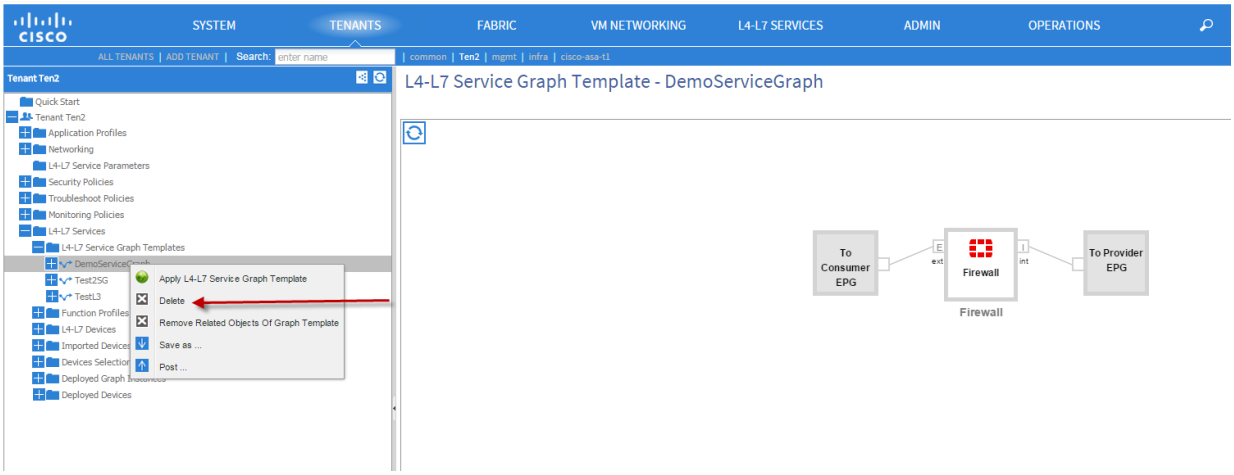
2. Select ***Contract and Provider EPG*** from the drop down list and check all 3 boxes:
   - ***Remove Related Contract***
   - ***Remove Related EPG Parameters***
   - ***Remove Related Device Selection Policies***

Hit *Submit*. This will remove all the related objects for this Service Graph.



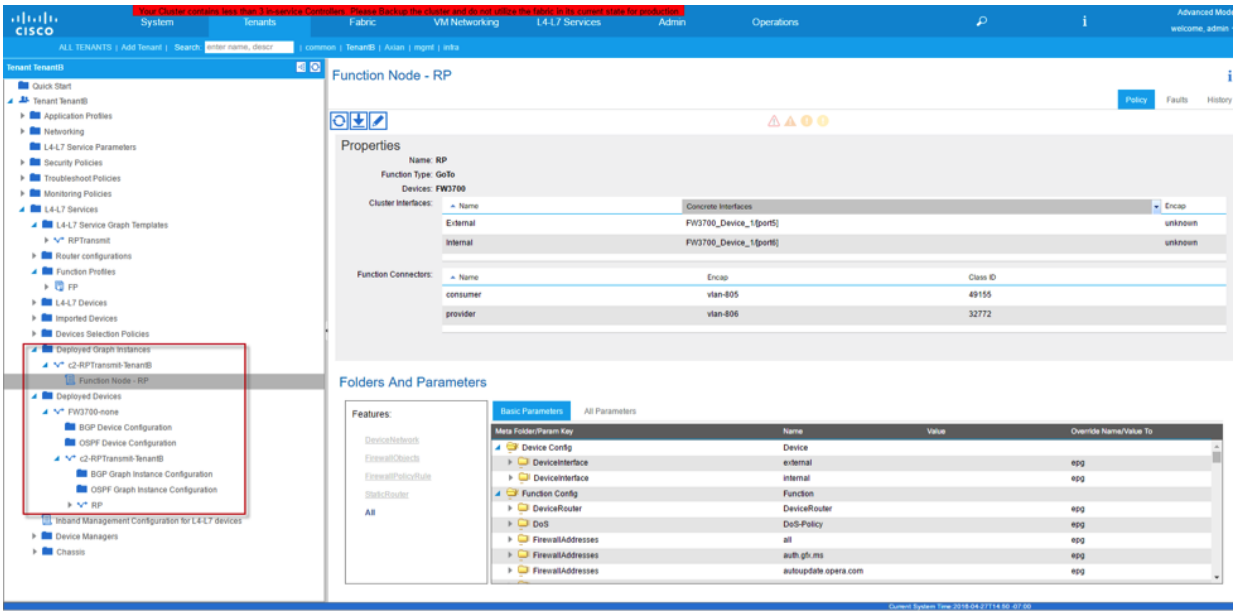
Delete the Service Graph

1. To delete the Service Graph Template, navigate to ***Tenant > L4-L7 Services > L4-L7 Service Graph Templates***.
2. Right click on template name listed on the left hand panel and select ***Delete*** option.



Service Graph deployed

Once the service graph is deployed, the Fortigate device will received configuration through REST API commands from the Cisco APIC. Below figure shows a successful service graph deployment. The Interface configuration such as vlan, IP..etc and firewall policies are all being programmed onto the Fortigate. From this point forward, any update is continue to be manage by Cisco APIC until the service graph is remove.



Installation Variations

Deploying Data Center Layer 2 Segmentation with Cisco ACI and FortiGate

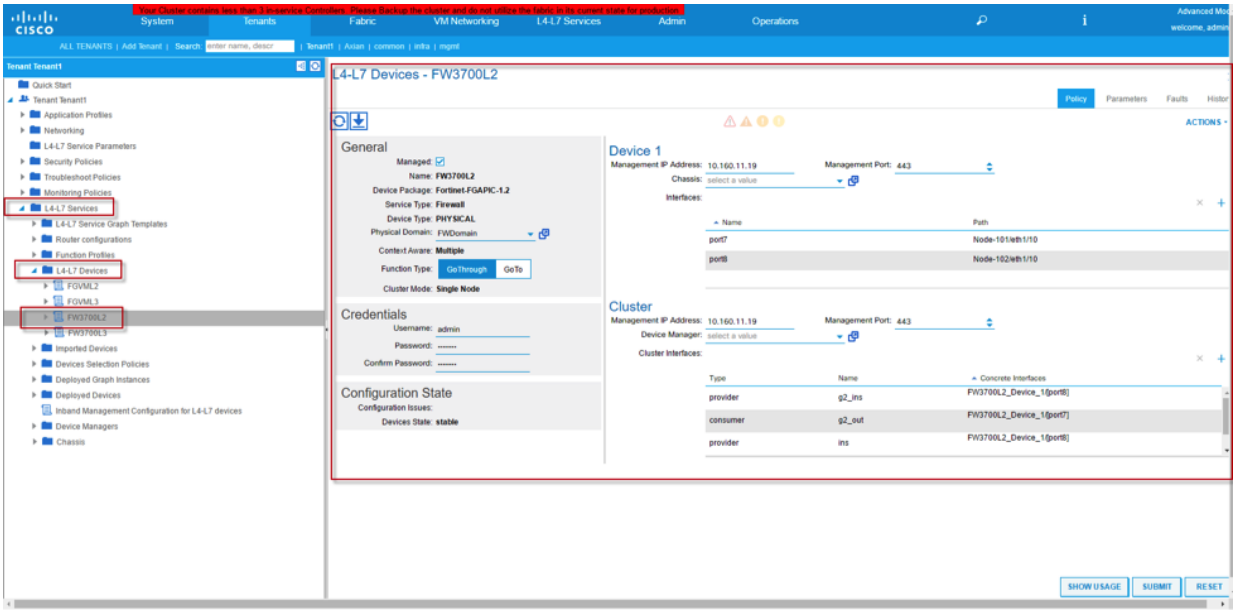
Pre-requisites

- Fabric Access Policies creation relating to
  - Vlan Pools
  - Domain
  - Attachable Access Entity Profiles
  - Interface Policies
  - Switch policies
- Create Tenant, VRF, 2 Bridge Domains, 2 EPGs
- Associate 2 Bridge Domains to VRF
- Associate 2 EPGs to the 2 Bridge Domains
- Layer 4-7 Device Package has imported into Cisco APIC

Work Flow:

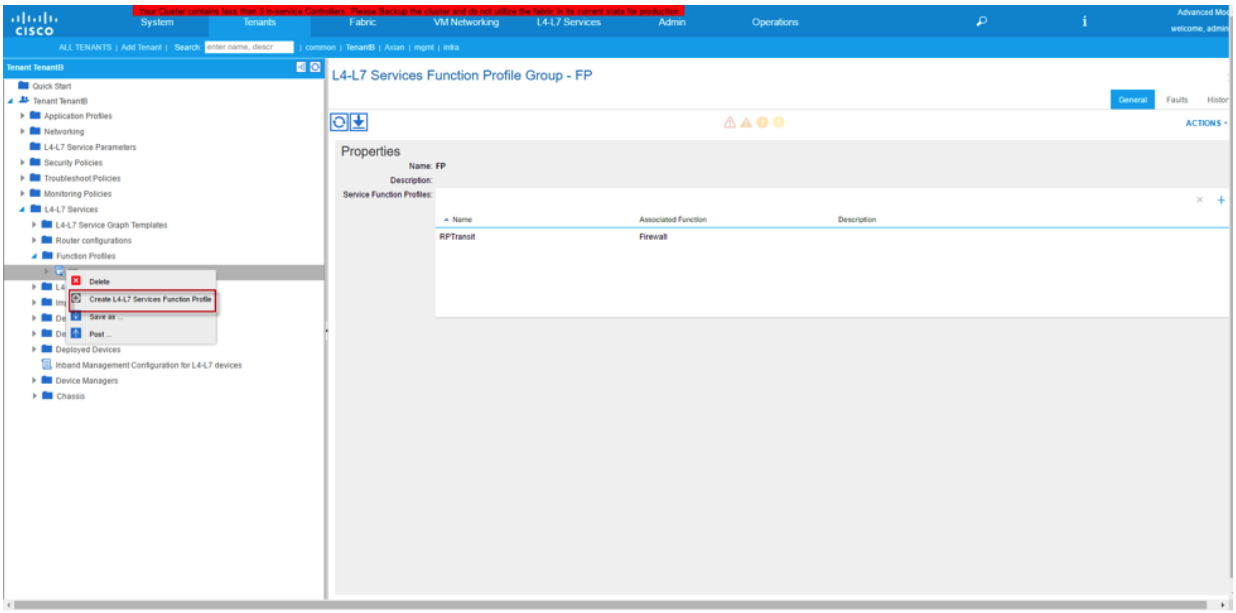
1. Create L4-L7 Device with Go-through Mode
2. Create Functional Profile
3. Create Service Graph Template
4. Deploy Service Graph

Create L4-L7 Device with Go-Through mode on Cisco APIC



Create Functional Profile

Functional Profile defines the template for the Service(s) that is going to deploy, such as L4-L7 Device Interface IP addresses, Rule ID, Object Addresses, Policy Rules, Source/Destination Ports…etc.



Functional Profile Objects Explanation under “Features”:

Device Network

Contained External and Internal Interfaces that will be programmed onto Fortigate VDOM. This is the interfaces (typically external and internal) that will be associated to the VDOM. If user intends to have multiple legs deployment scenario, this is where he/she can add additional interfaces with unique name.

User must leave IP address field untouched in Go-through mode.

Firewall Objects

This field allows user to customize Firewall Addresses, Service and scheduling.

Firewall Policy Rule

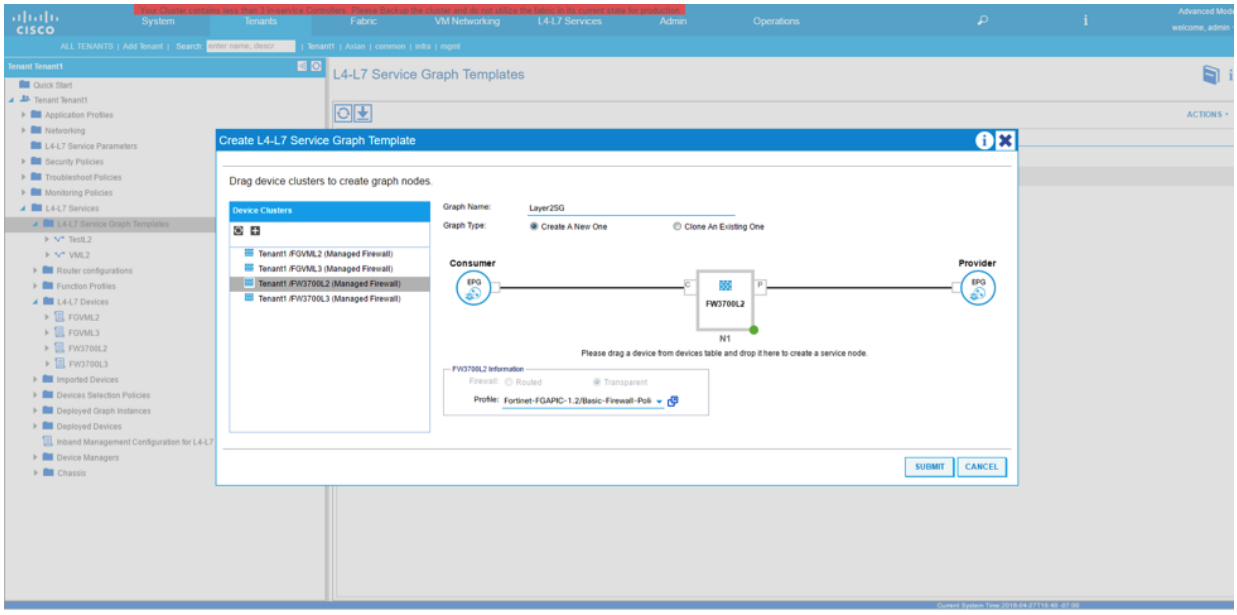
This field encompassed the creation of Firewall policy that will be program onto Fortigate. Security Profile and Logging Options are also configured here.

All

This field listed all the parameters stated above plus DDOS configuration.

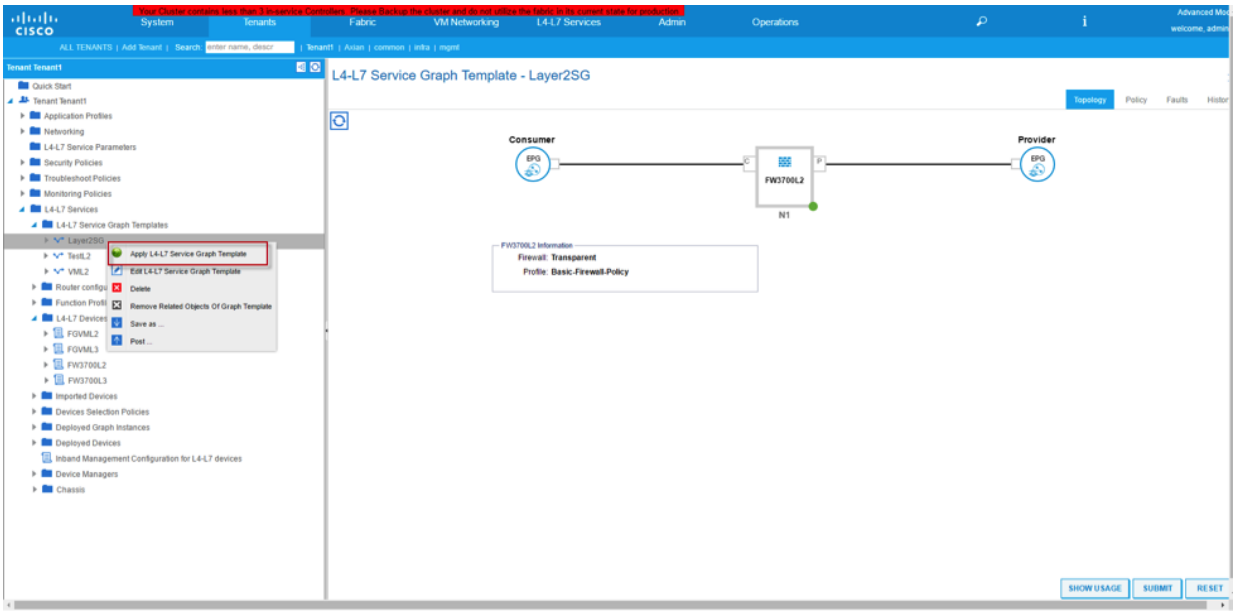
Create Service Graph

Service Graph template is used to tightly coupled the Functional Profile or Firewall configuration and combine with the Firewall device we defined at earlier steps.

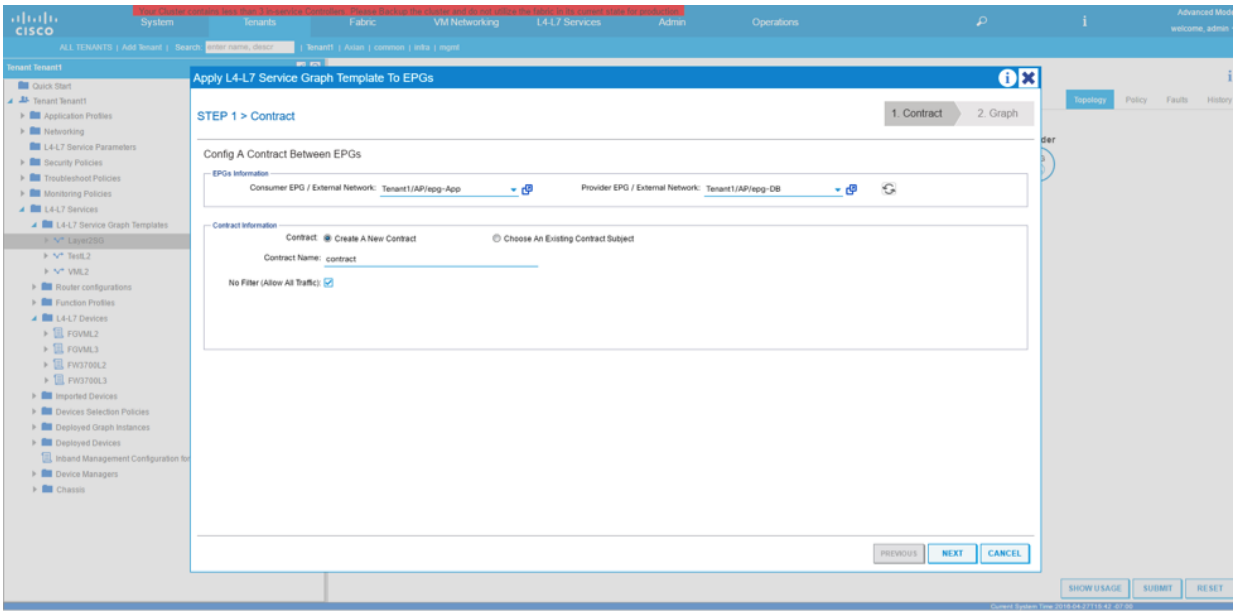


Deploy Service Graph

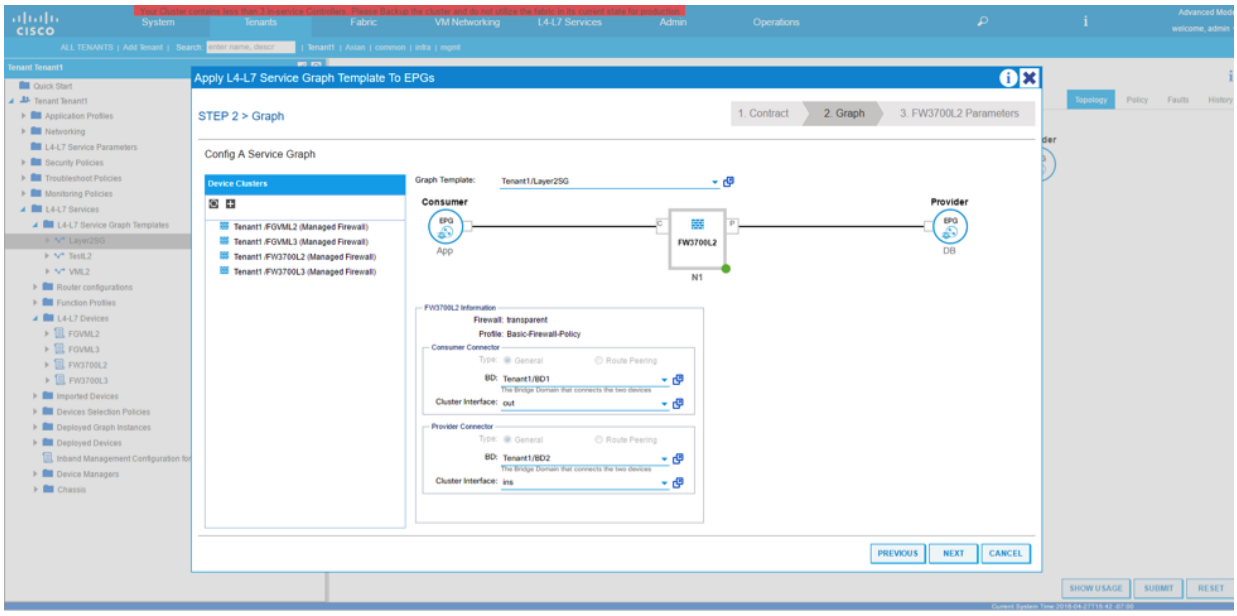
Once we combined the Firewall configuration and associated device together, we are ready to deploy the Service Graph.



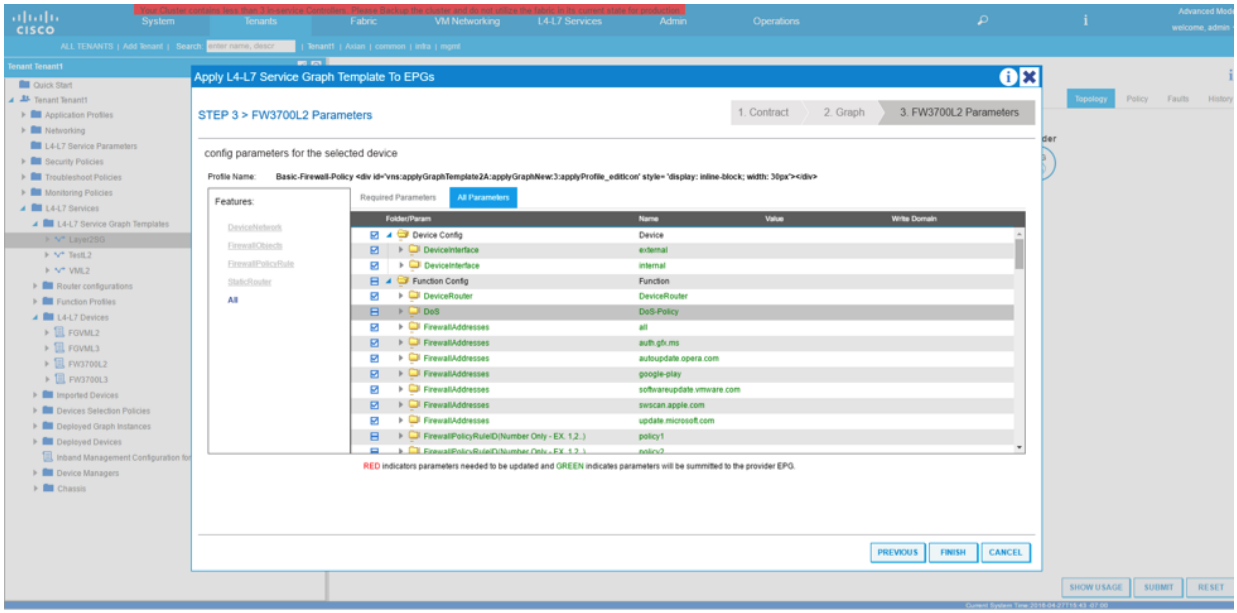
On next screen select the Consumer and Provider EPGs and assign a contract name or select a pre-define contract.



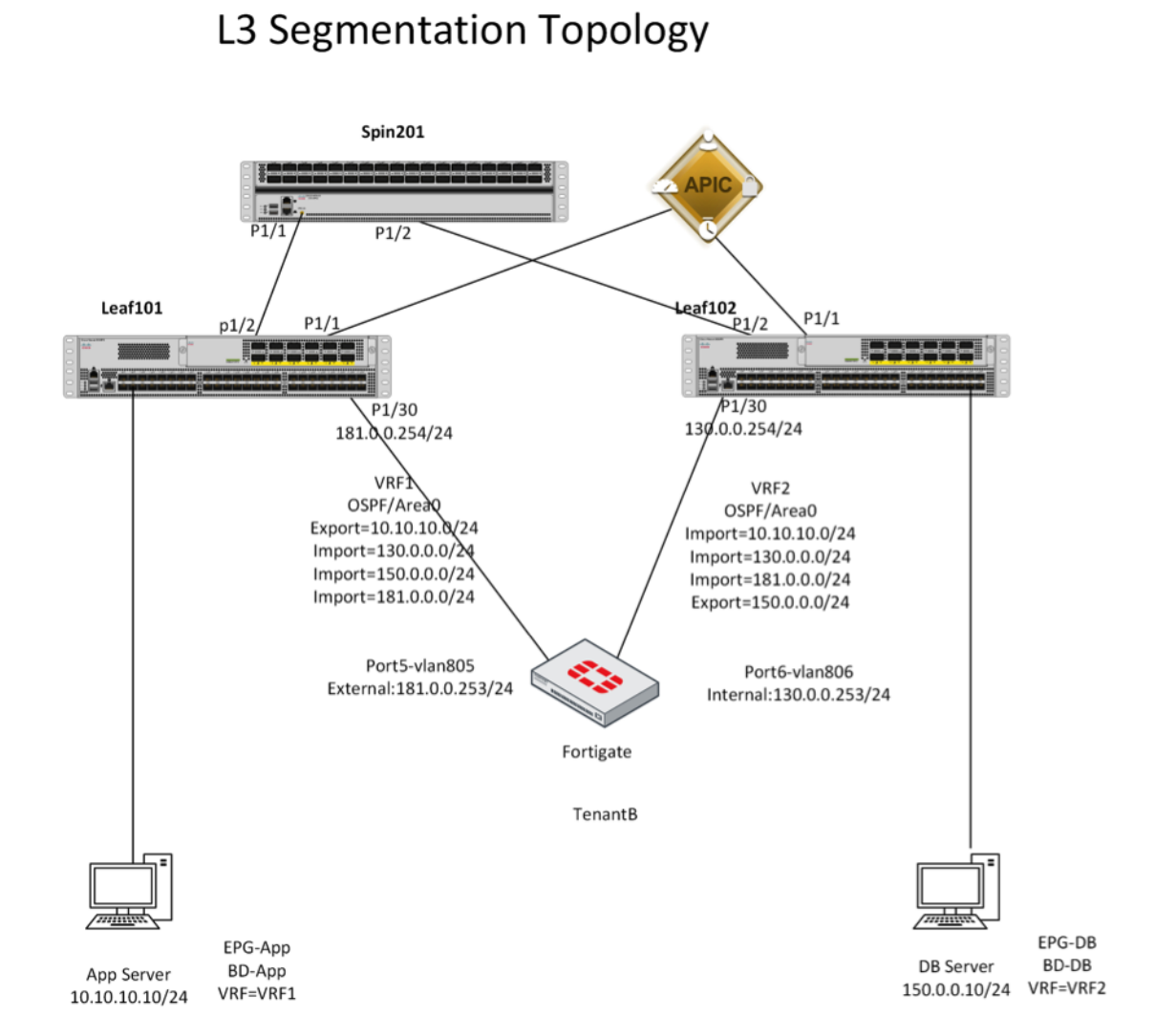
Next screen select the logical interfaces defined during the creation of L4-L7 Device.



Next screen is the last minute to validate all configurations before deploy, then hit the submit button.



Deploying Data Center Layer 3 Segmentation with Cisco ACI and FortiGate



Introduction:

This document describes the configuration walk through of L4-L7 Service Graph with L3 Segmentation within Data Center.

Prerequisites:

Please pre-configure below configuration before deploying this design:

- Fabric Access Policies creation relating to:
  - VLAN Pools
  - Domain

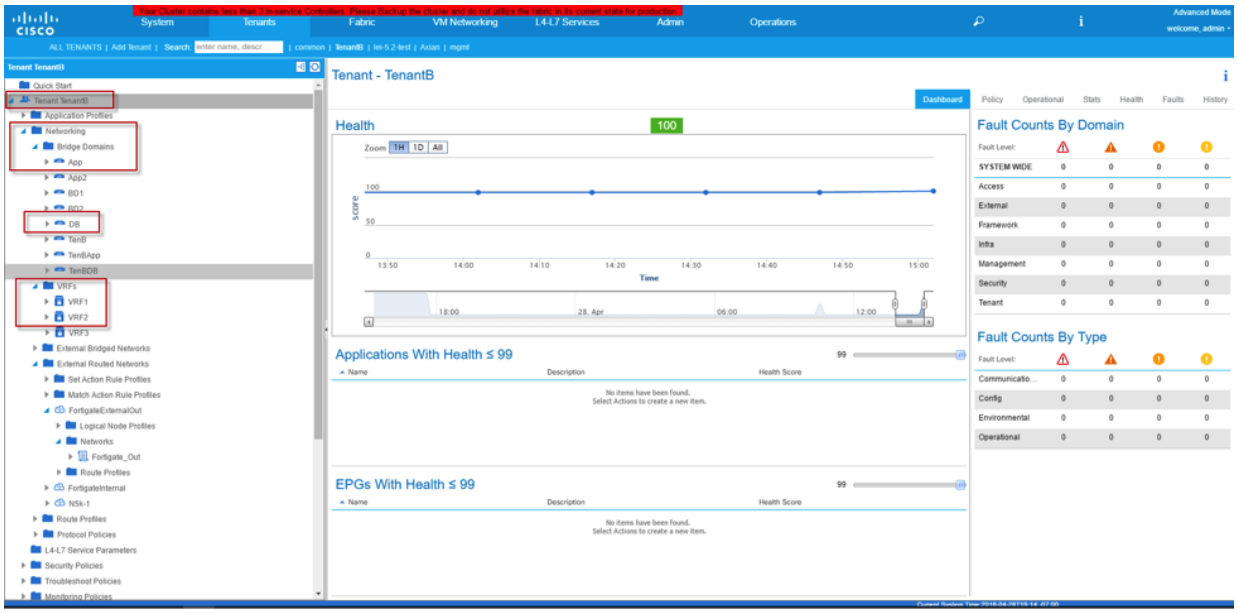
  - Attachable Access Entity Profiles
  - Interface Policies
  - Switch Policies
- L4-L7 Device Package has imported into Cisco APIC

Work Flow:

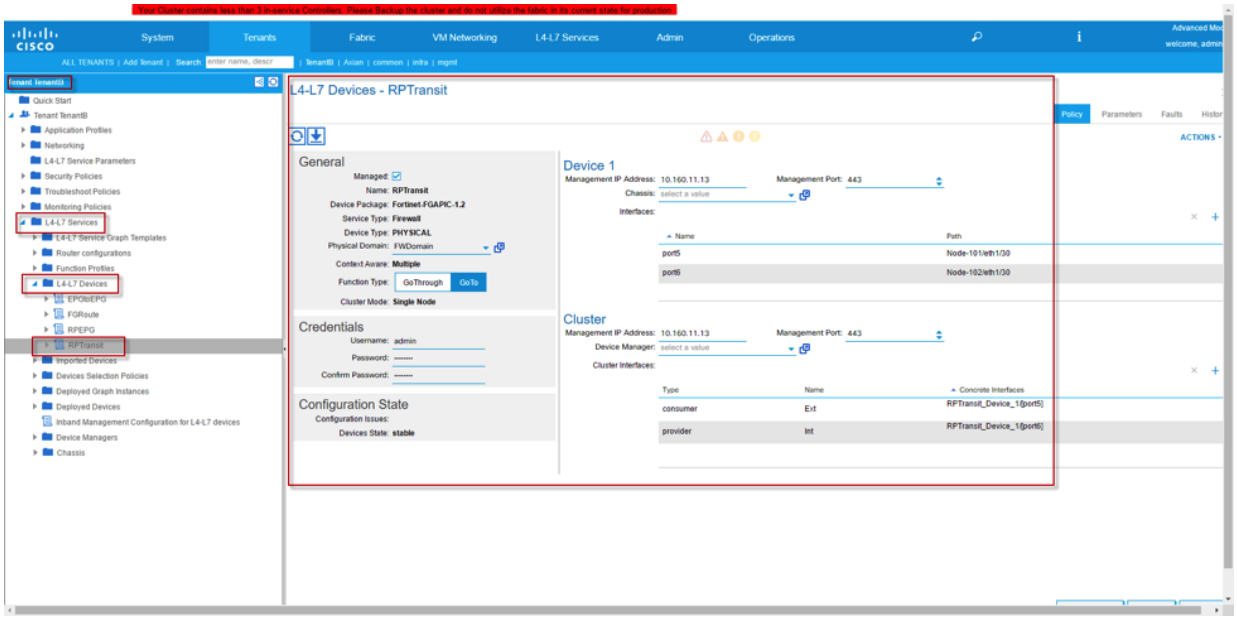
1. Create Tenant (TenantB in our example)
2. Create VRFs (VRF1 and VRF2 in our example)
3. Create Bridge Domains and map to VRFs (Bridge Domain App and DB are mapped to VRF1 and VRF2 respectively in our example)
4. Create EPGs and map to Bridge Domains (EPG-DB and EPG-App in our example)
5. Create two L3Out EPGs (1 for Firewall External and 1 for Firewall Internal. In our example, we created “FortigateExternalOut” for Firewall External and “FortigateInternal” for Firewall Internal)
6. Configure gateway IPs on Bridge Domains (DB and App) for App and DB Servers
7. Ensure “Unicast Routing” is checked in each Bridge Domain
8. In Bridge Domain App, associate L3Outs to “FortigateExternalOut”; in Bridge Domain DB, associate L3Outs to “FortigateInternal”
9. Map App and DB machines to EPGs and configure correct IP addresses, and use Bridge Domain IP address (configured in step 6) as its gateway
10. Verify App and DB machines can ping to gateway IP address
11. Create L4-L7 Device with GoTo mode
12. Create Functional Profile Group as well as Functional Profile
13. Create Route Profiles
14. Create L4-L7 Service Graph Template
15. Deploy L4-L7 Service Graph

Configuration:

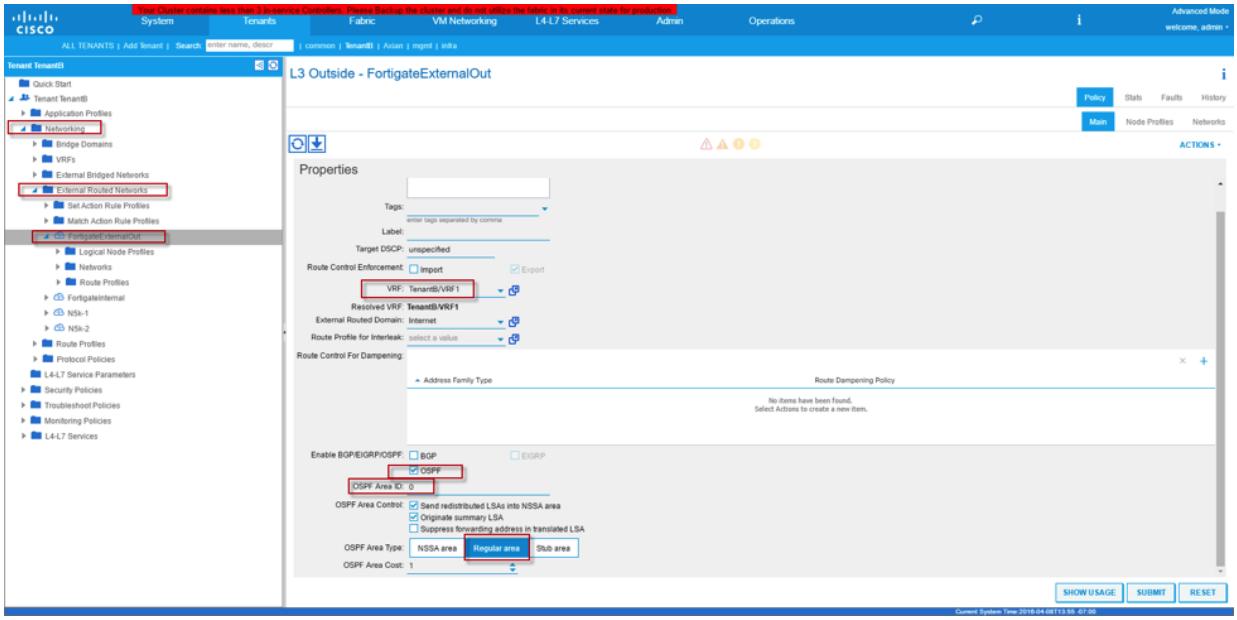
Configure the Bridge Domain DB and App as well as VRF1 and VRF2. Associate Bridge Domain App to VRF1 and Bridge Domain DB to VRF2.



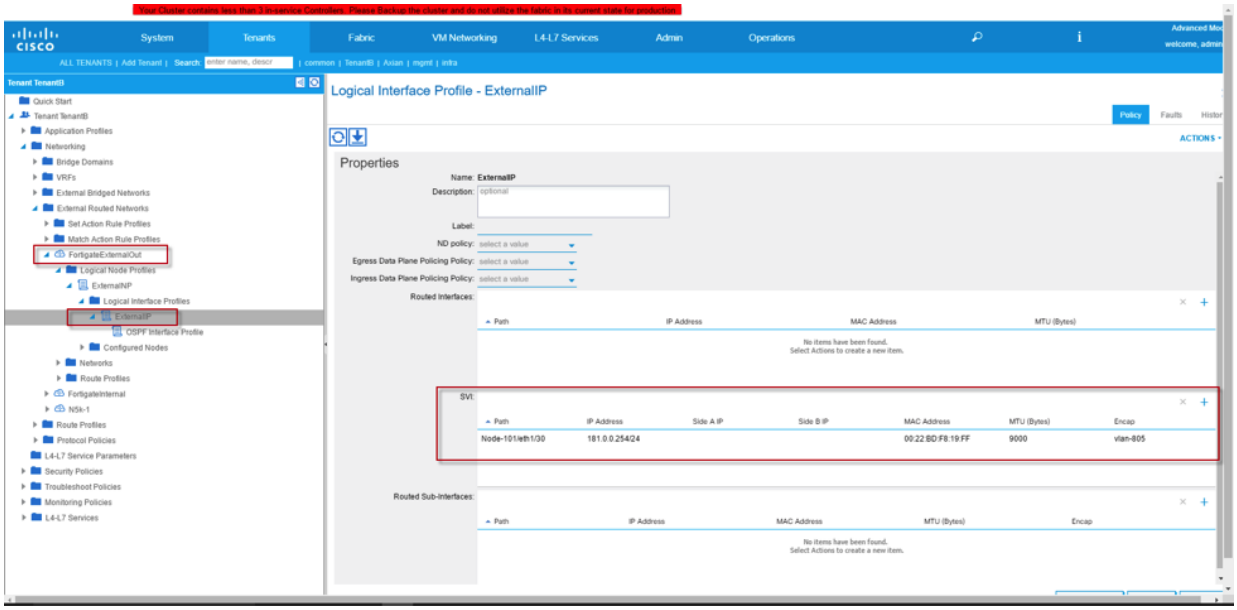
Configure L4-L7 Device for physical Fortigate (GoTo Mode)



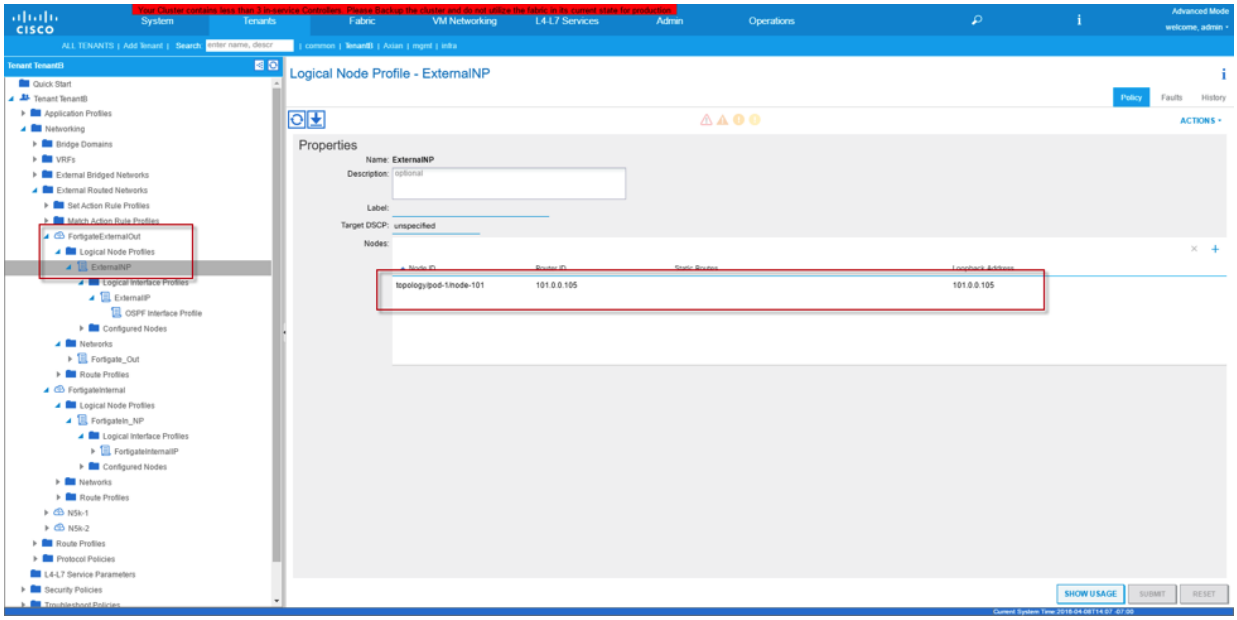
Configure L3Out for Fortigate External Interface and associate with VRF1



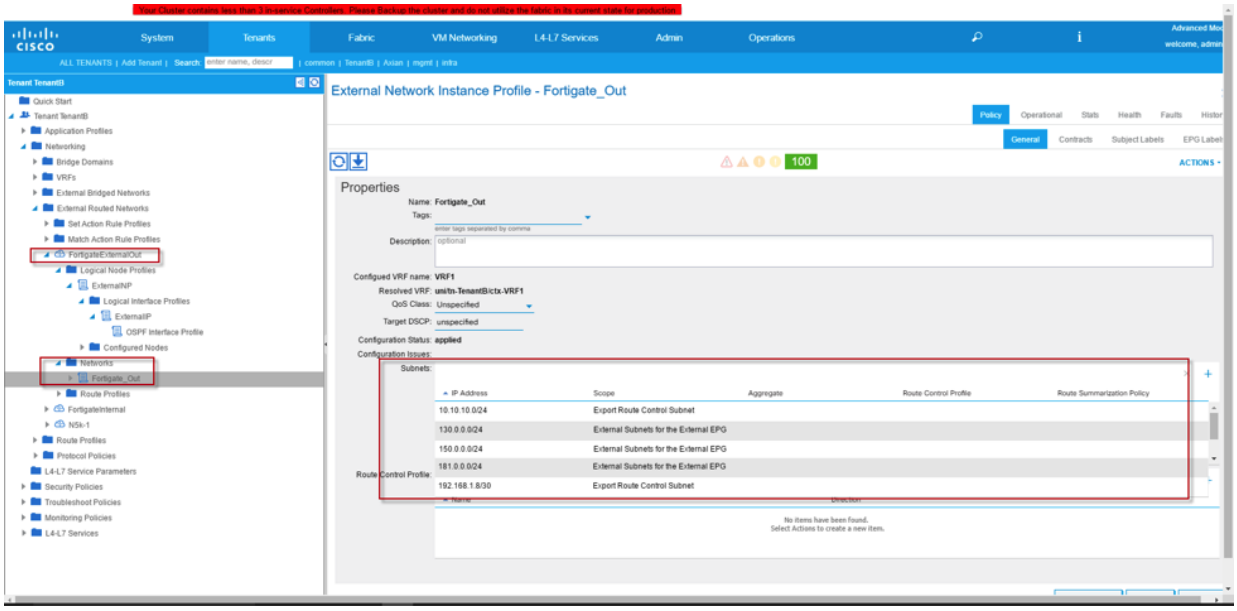
Configure SVI for L3Out Fortigate External out



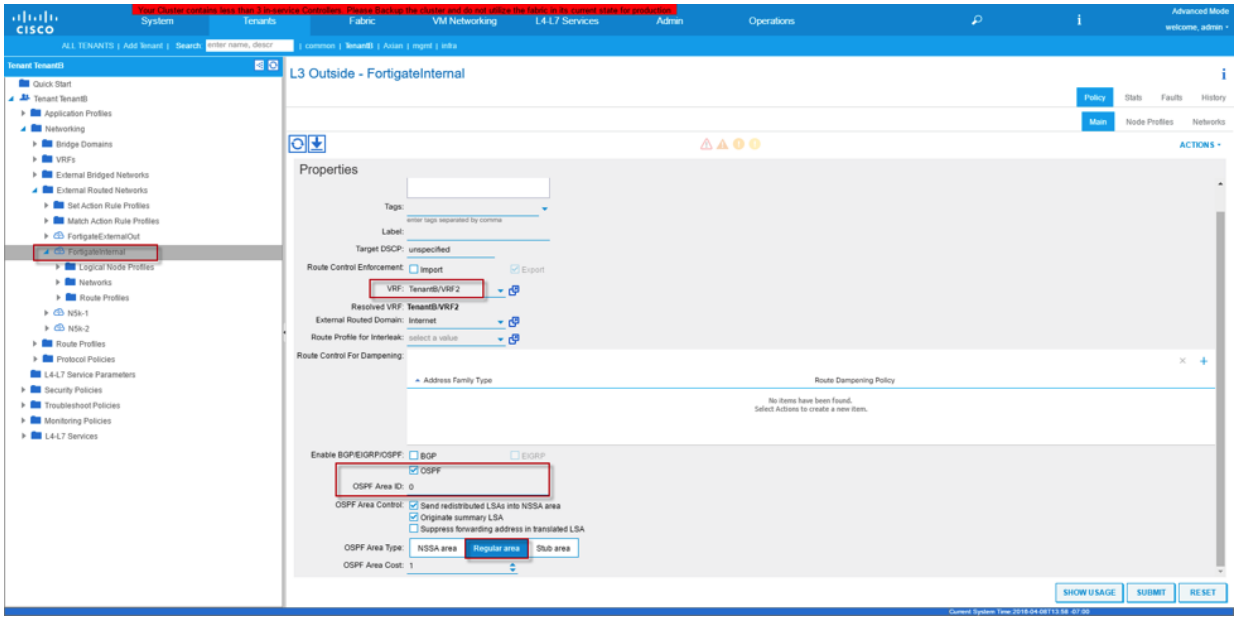
Configure Route ID for L3Out Fortigate External Out



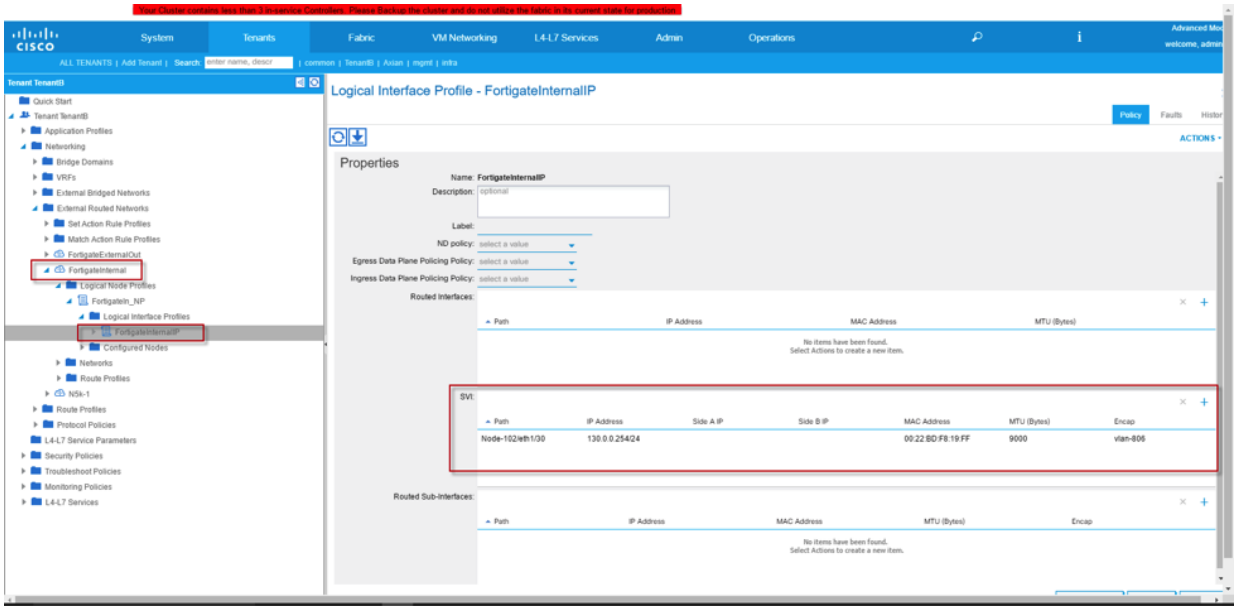
Configure Import/Export Route Control on Subnets for Fortigate External out



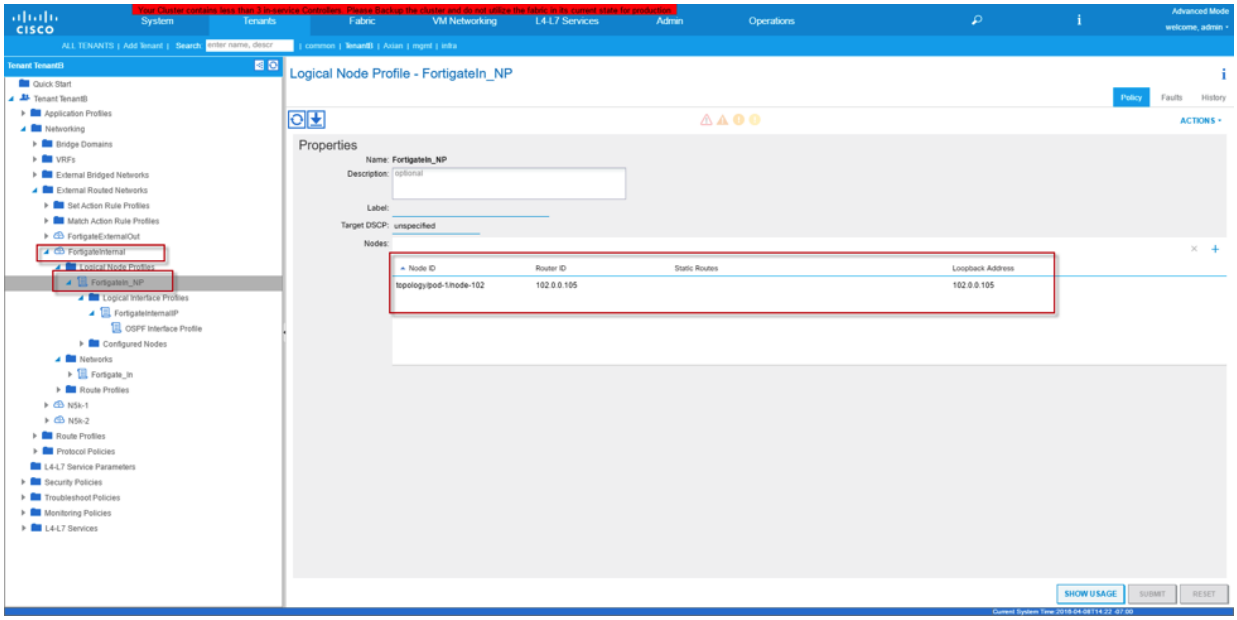
Configure L3Out for Fortigate Internal and associate with VRF2



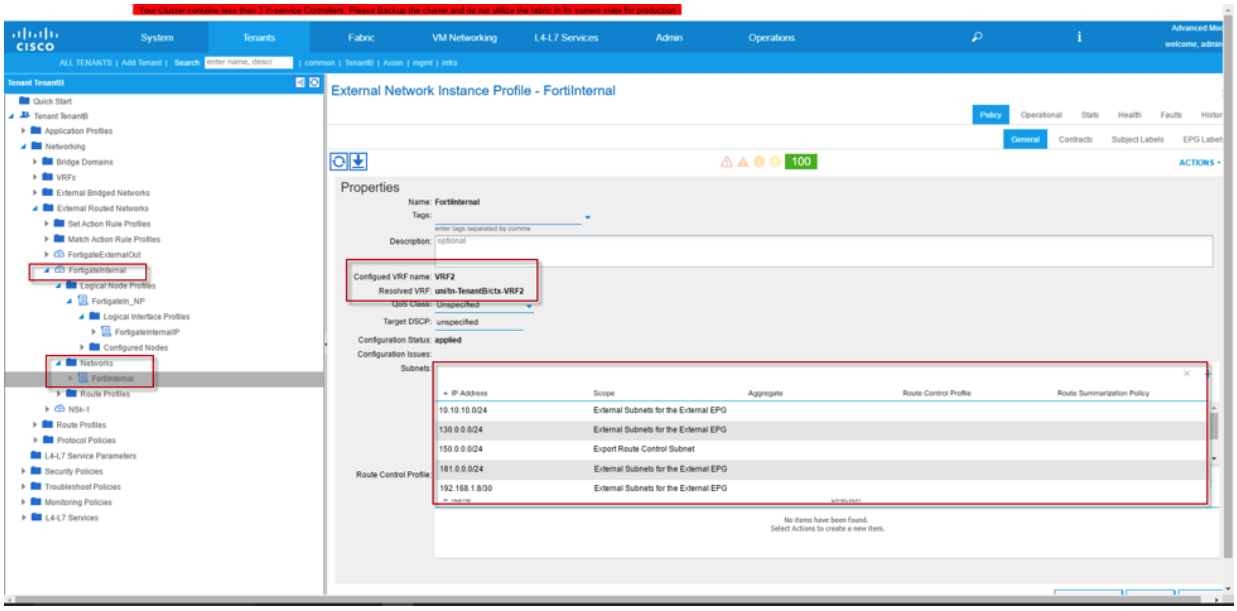
Configure SVI for L3Out Fortigate Internal



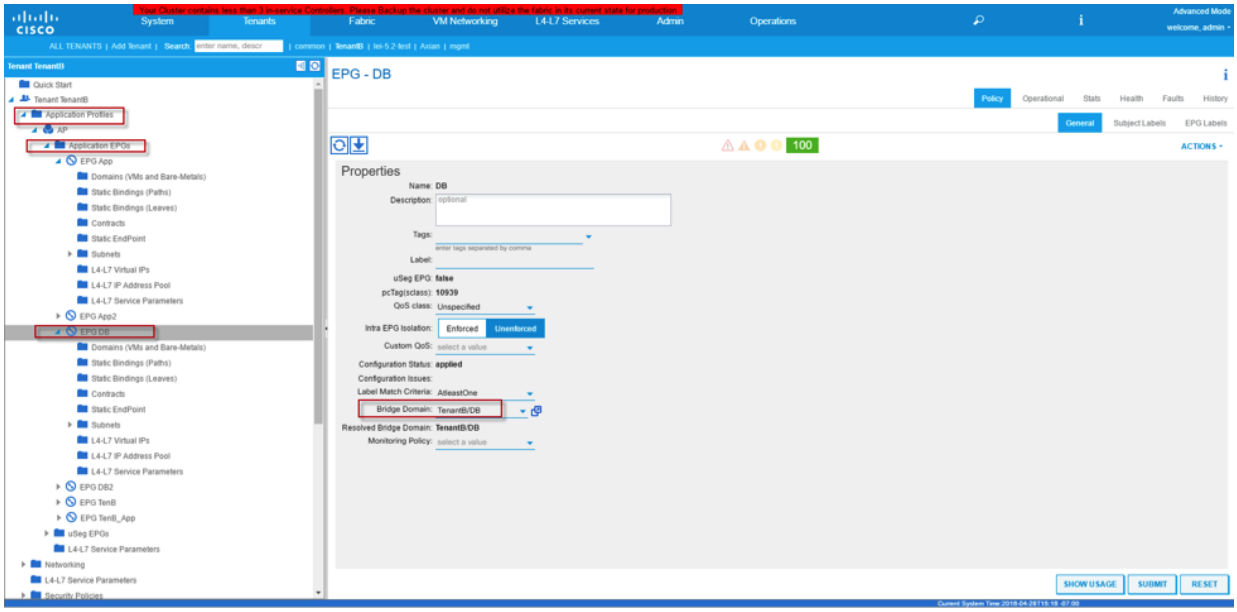
Configure Route ID for L3Out Fortigate Internal

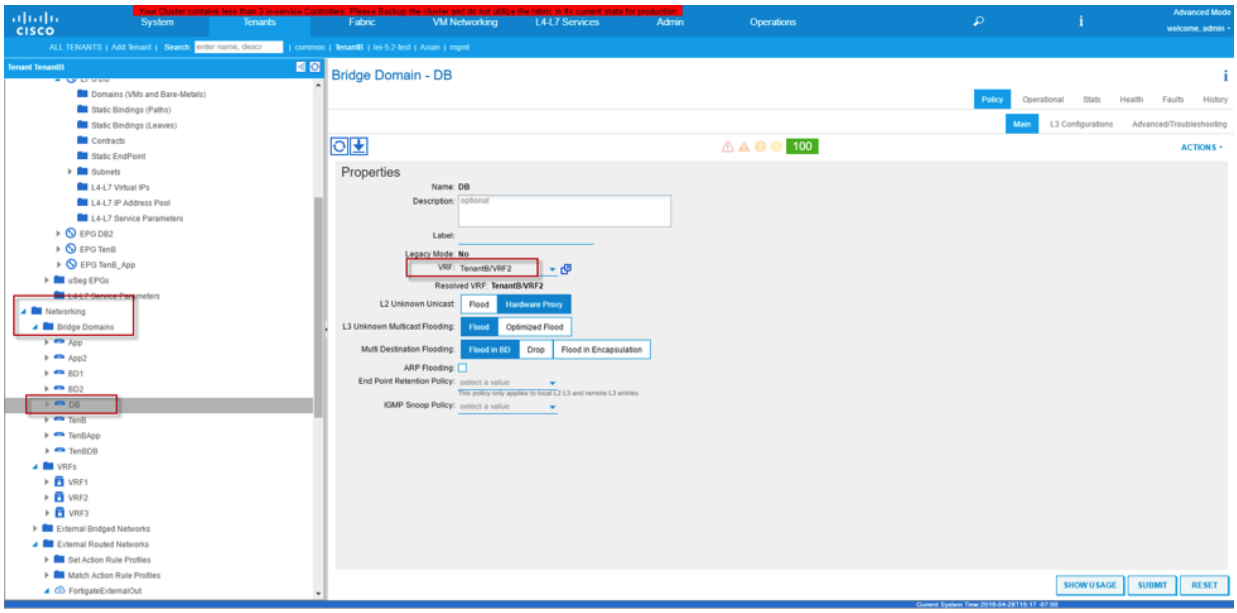


Configure Import/Export Route Control on Subnet for L3Out Fortigate Internal

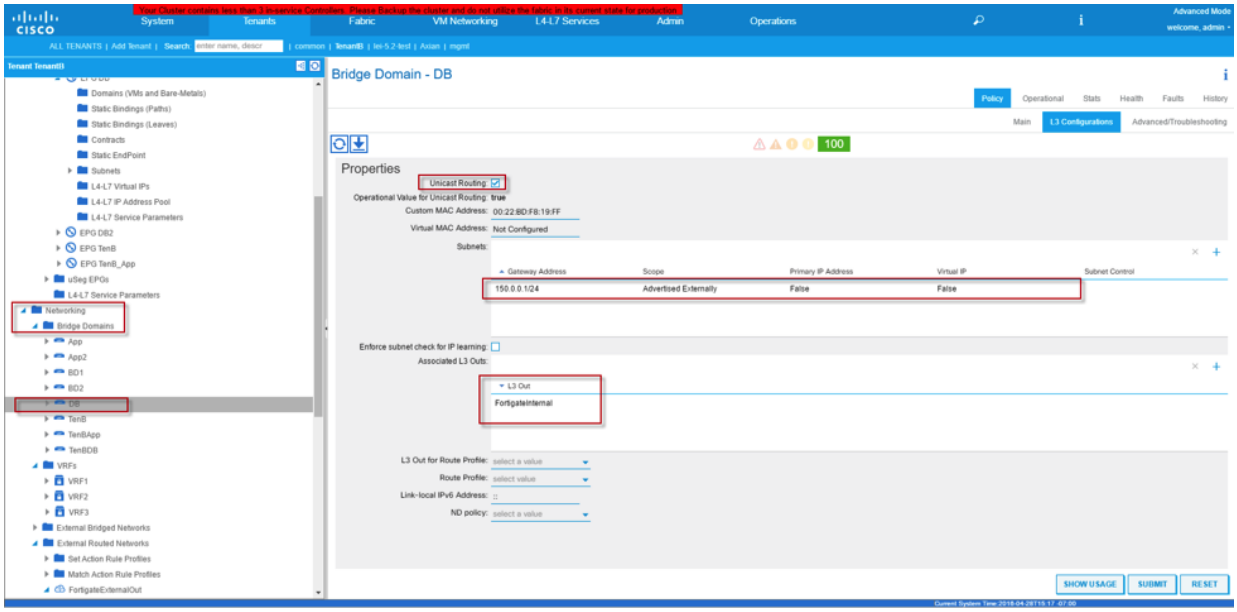


Associate EPG “DB” to Bridge Domain “DB” and attach Bridge Domain to VRF2

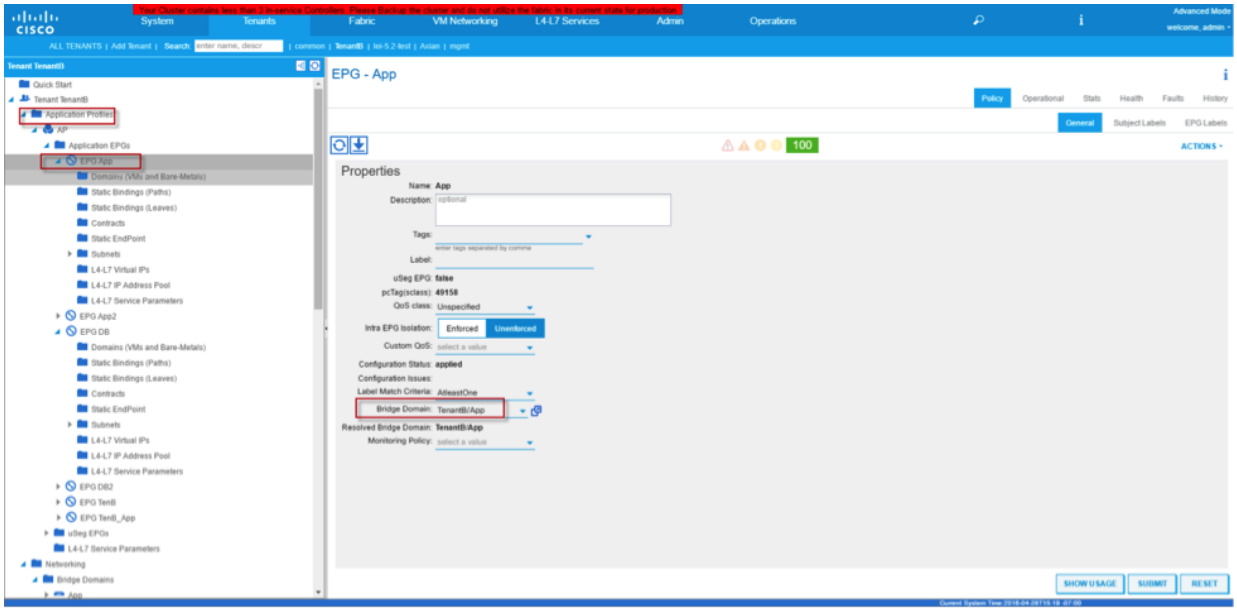


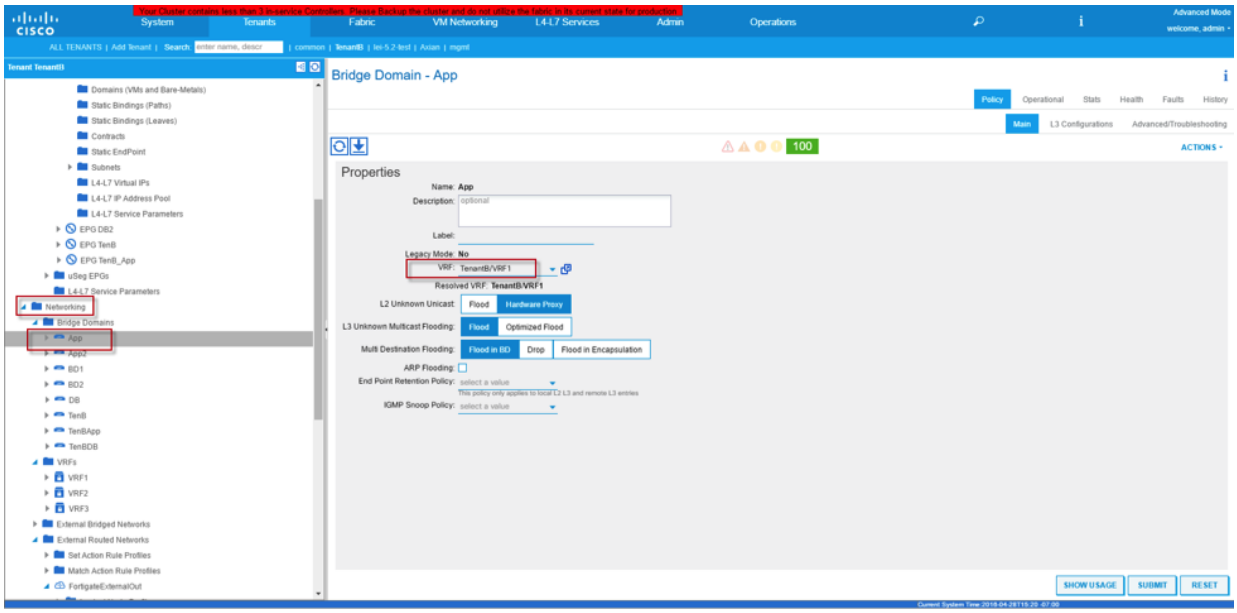


Configure Bridge Domain with Unicast Routing, assign SVI and associate L3Out to “FortigateInternal”

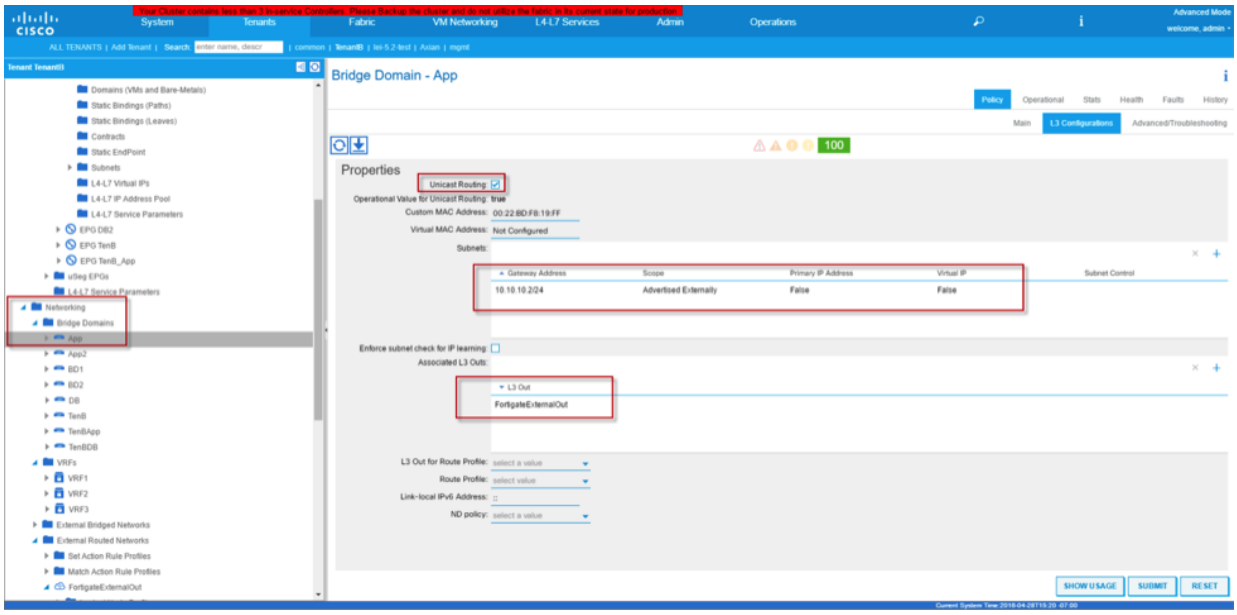


Associate EPG “App” to Bridge Domain “App” and attach Bridge Domain to VRF1

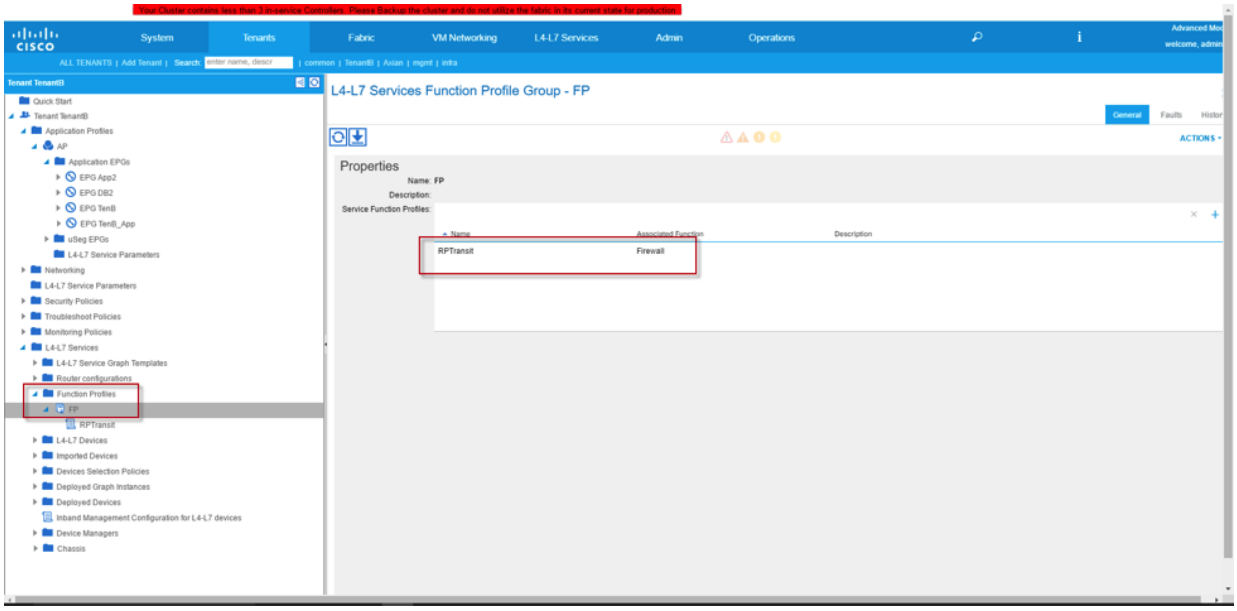


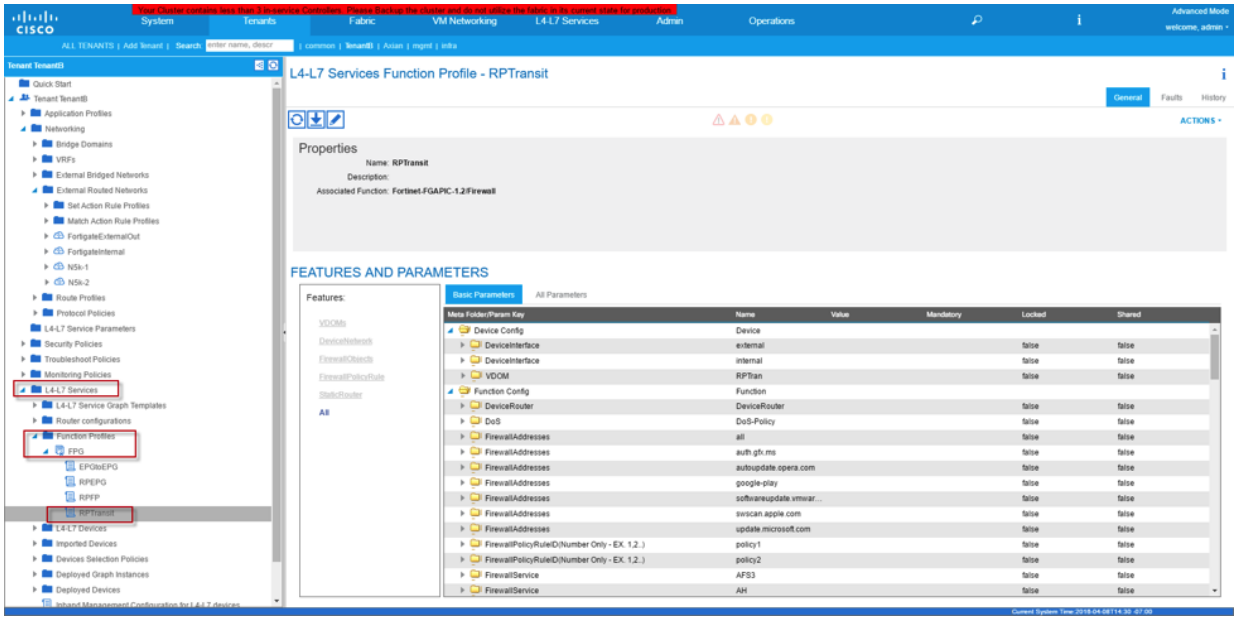


Configure Bridge Domain with Unicast Routing, assign SVI and associate L3Out to "FortigateInternal"

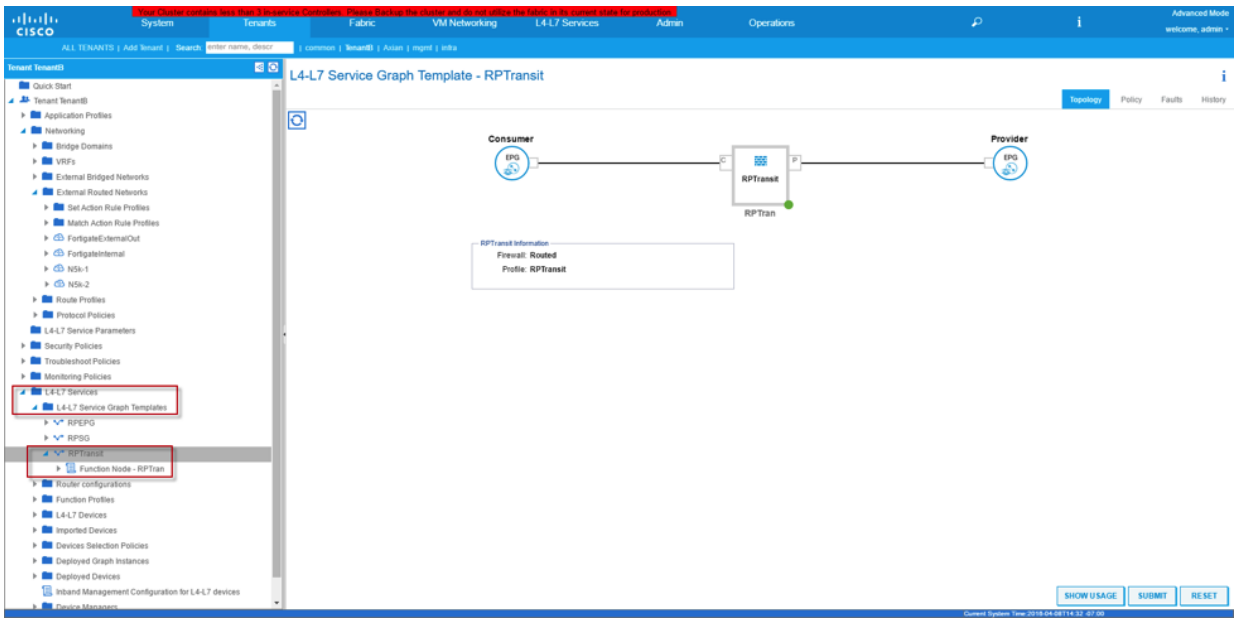


Create Functional Profile Group and Functional Profile from existing template

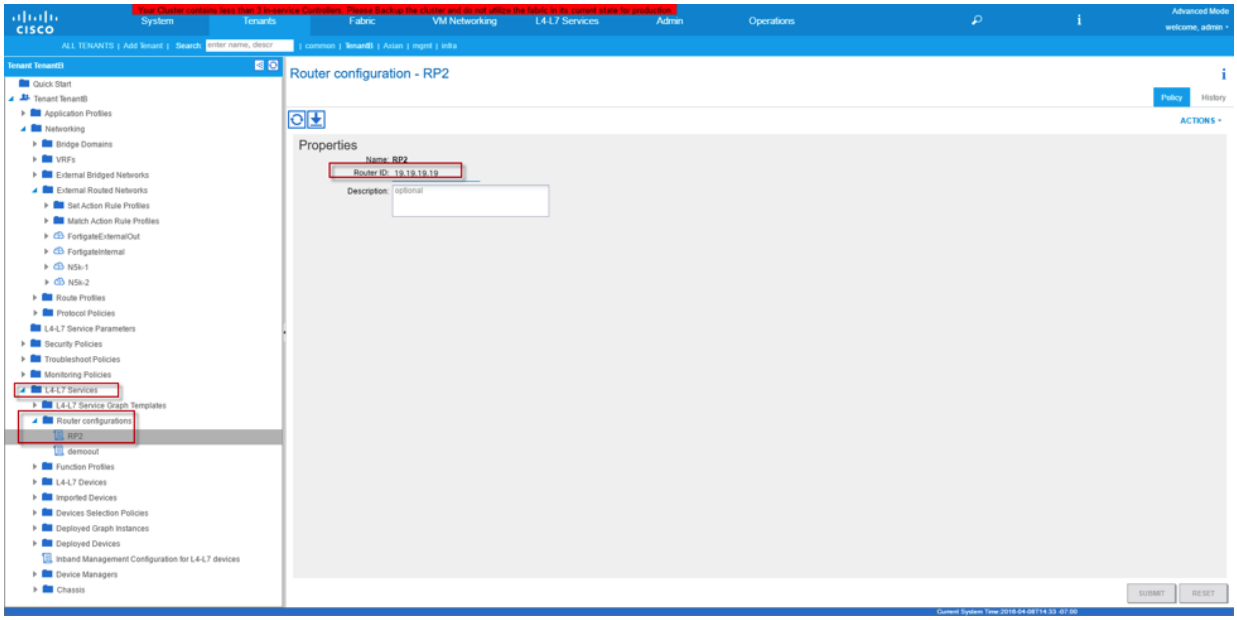




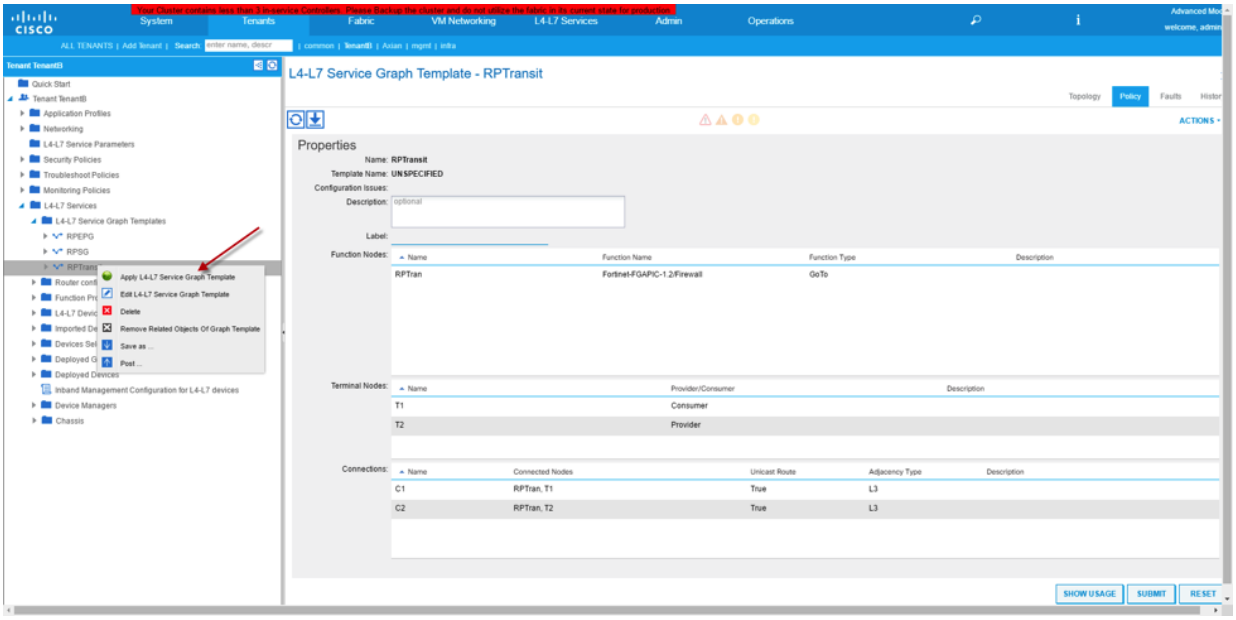
Create Service Graph template



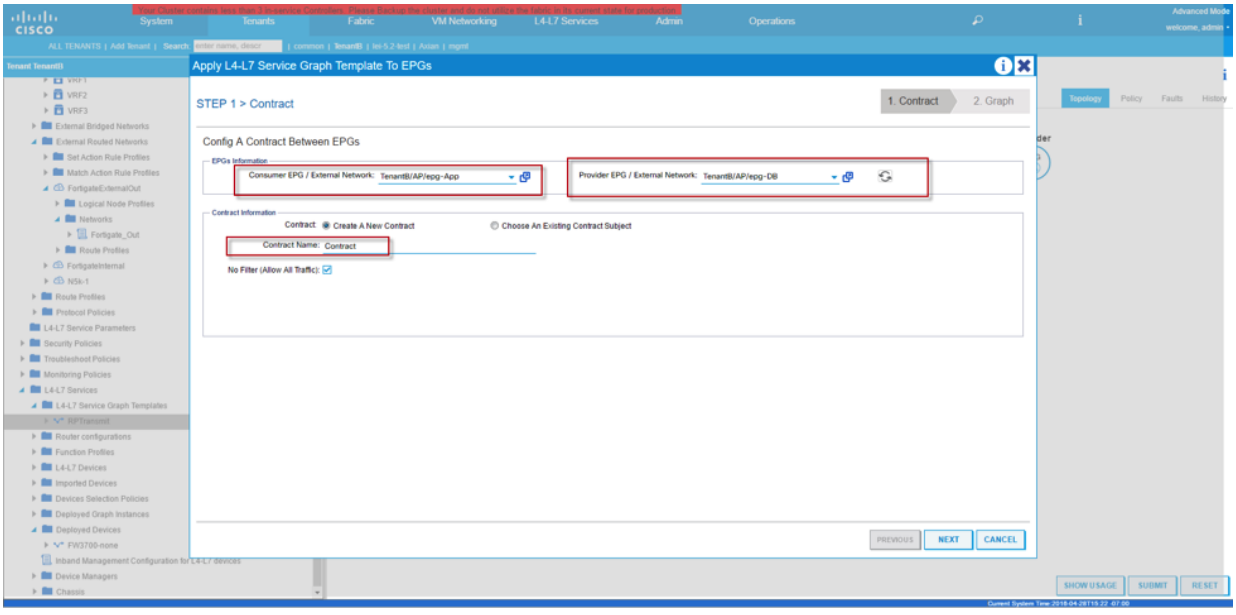
Create Router ID that will be used on the Service Appliance (Fortigate)



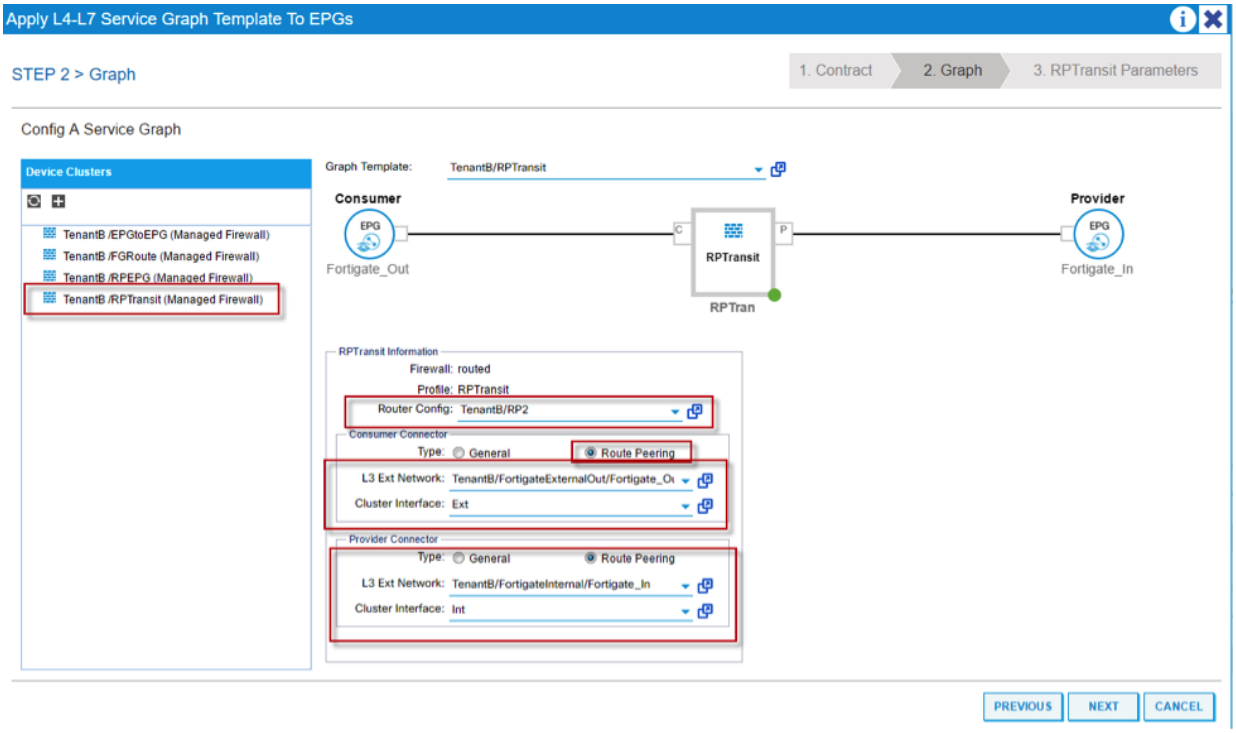
Deploy Service Graph



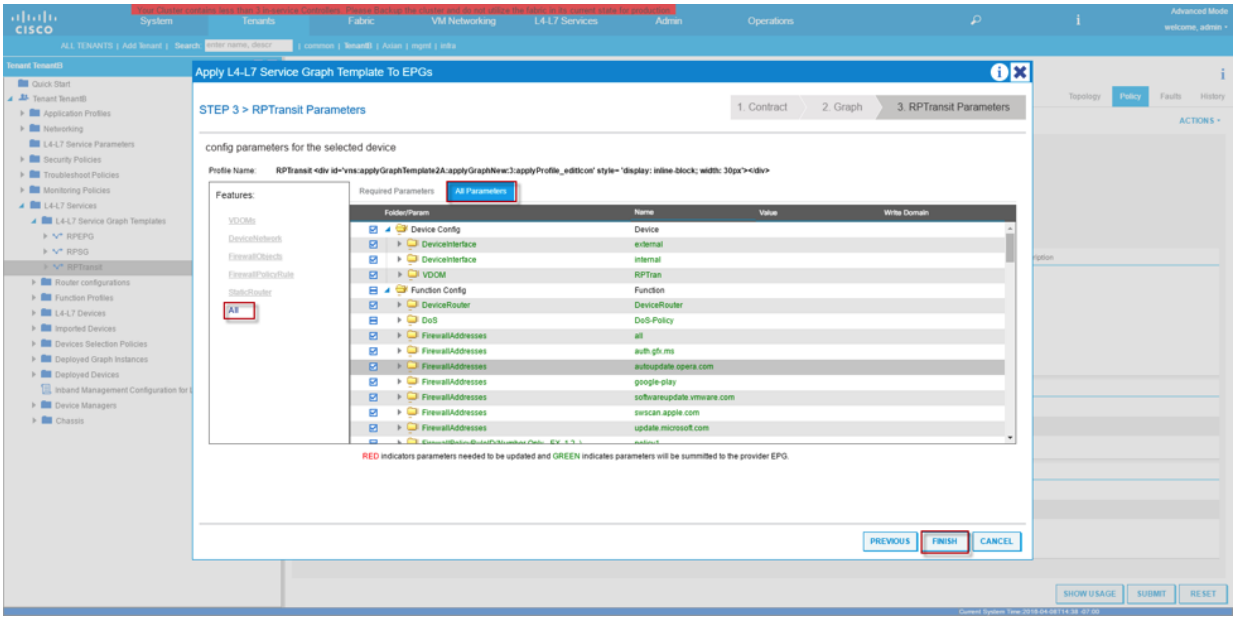
Consumer will be App EPG. Provider is the DB EPG.



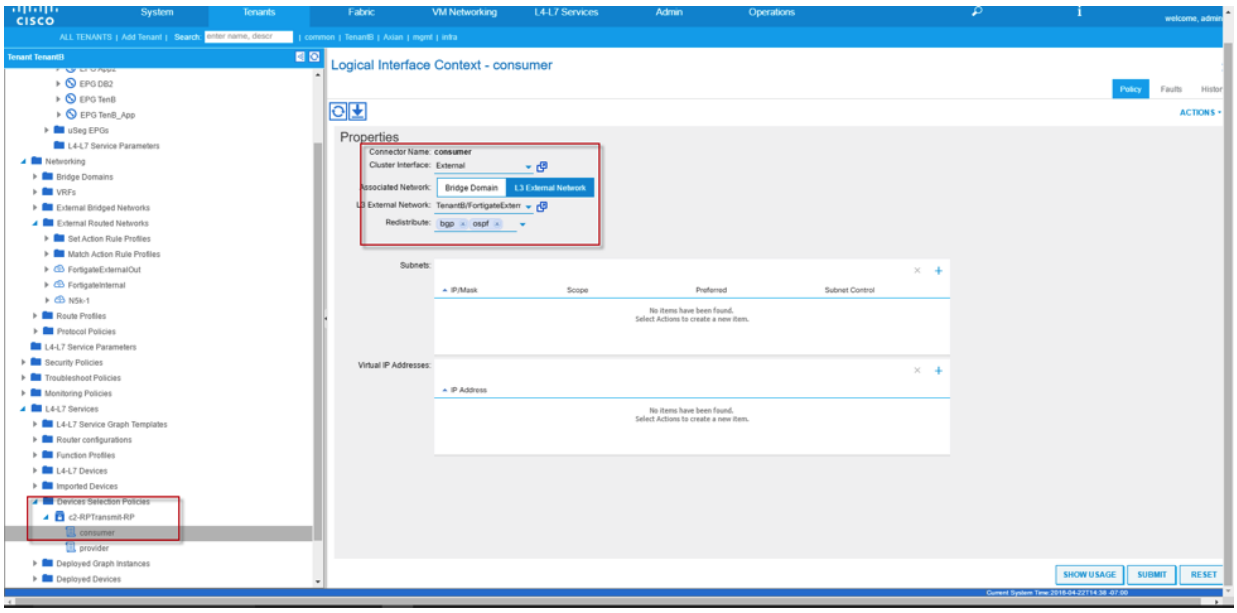
Please select for Internal and external connections. In our example, we used “FortigateExternalOut” and FortigateInternal” as External and Internal selections respectively.

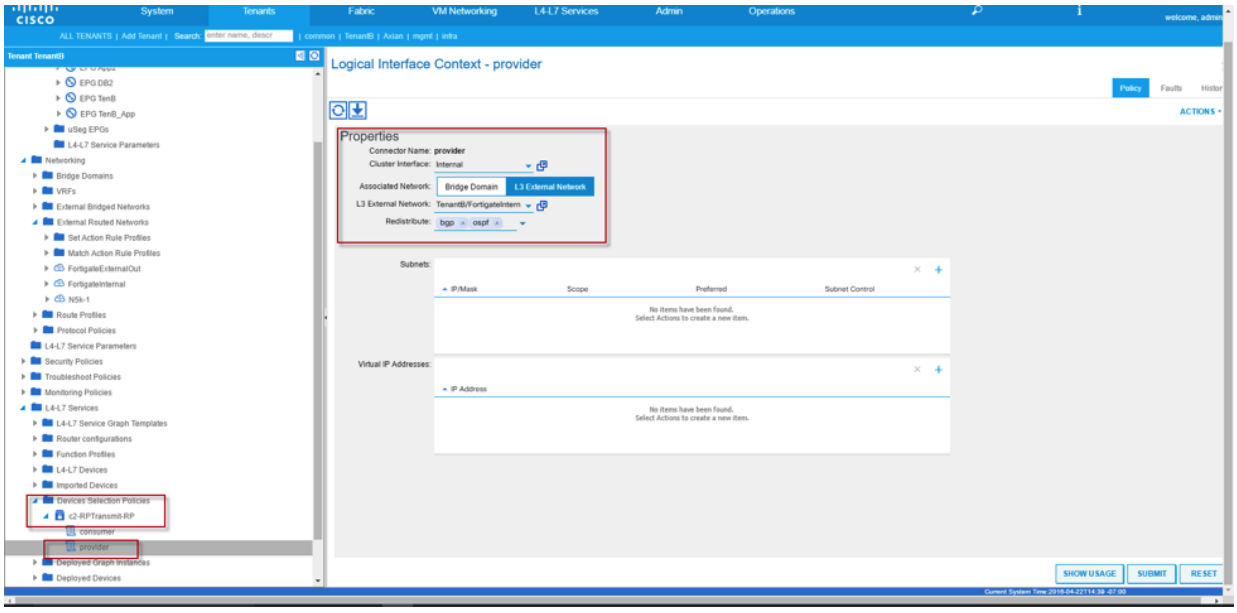


Last minute check to make sure configuration is good before hit “Finish” button

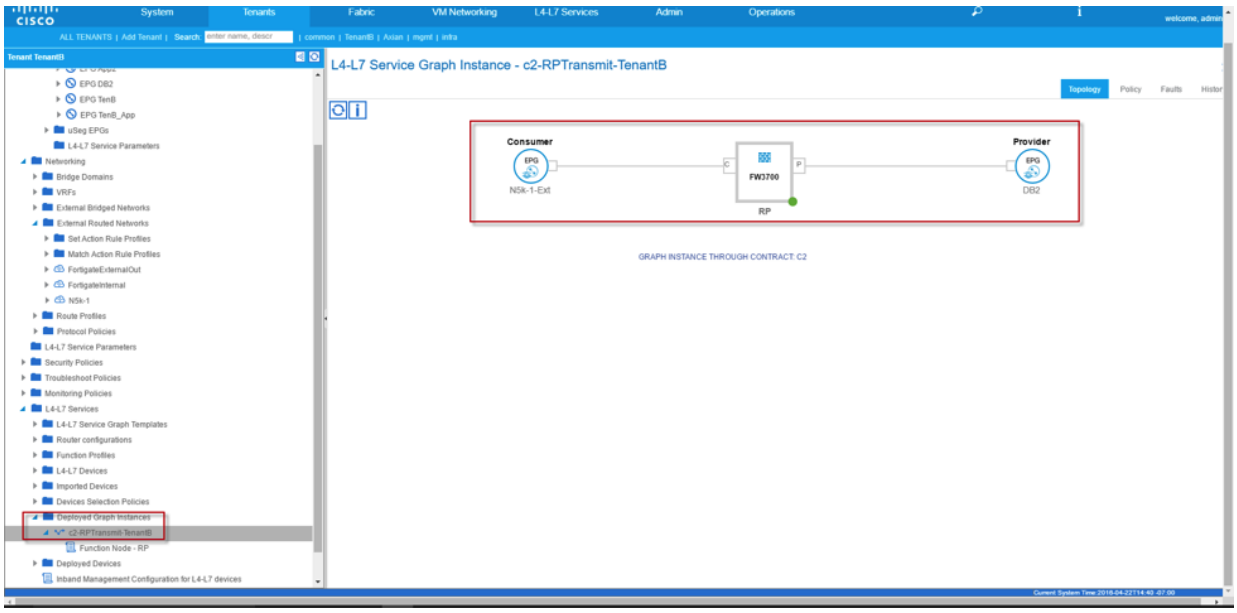


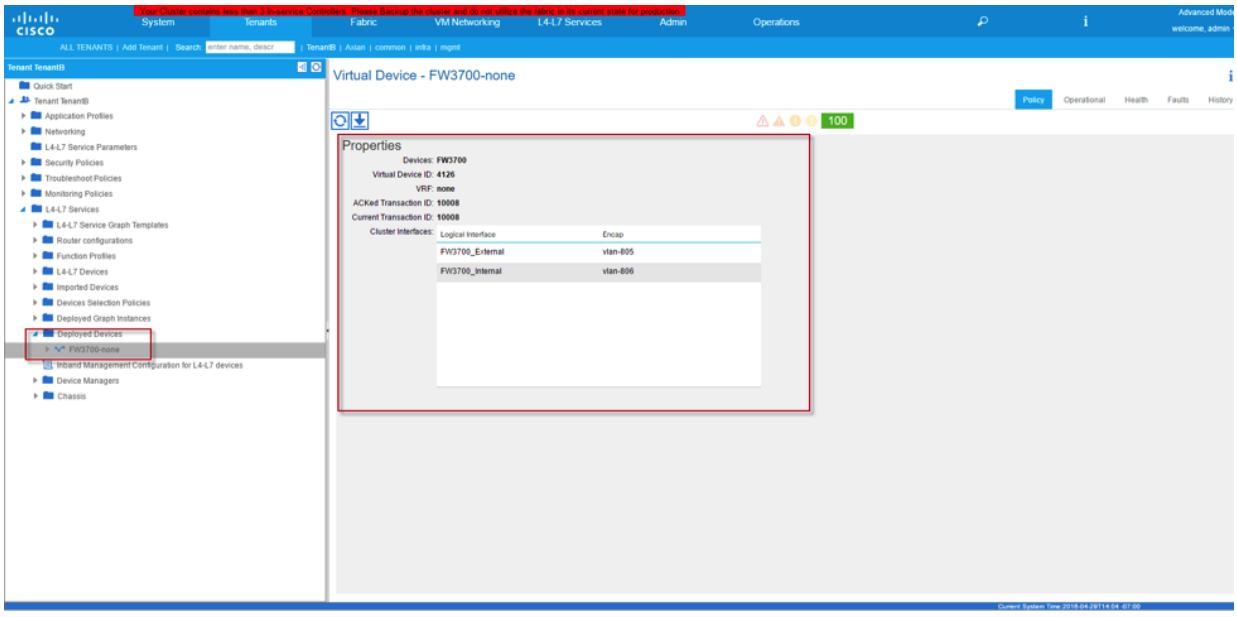
Check the status and verify Device Selection Policy



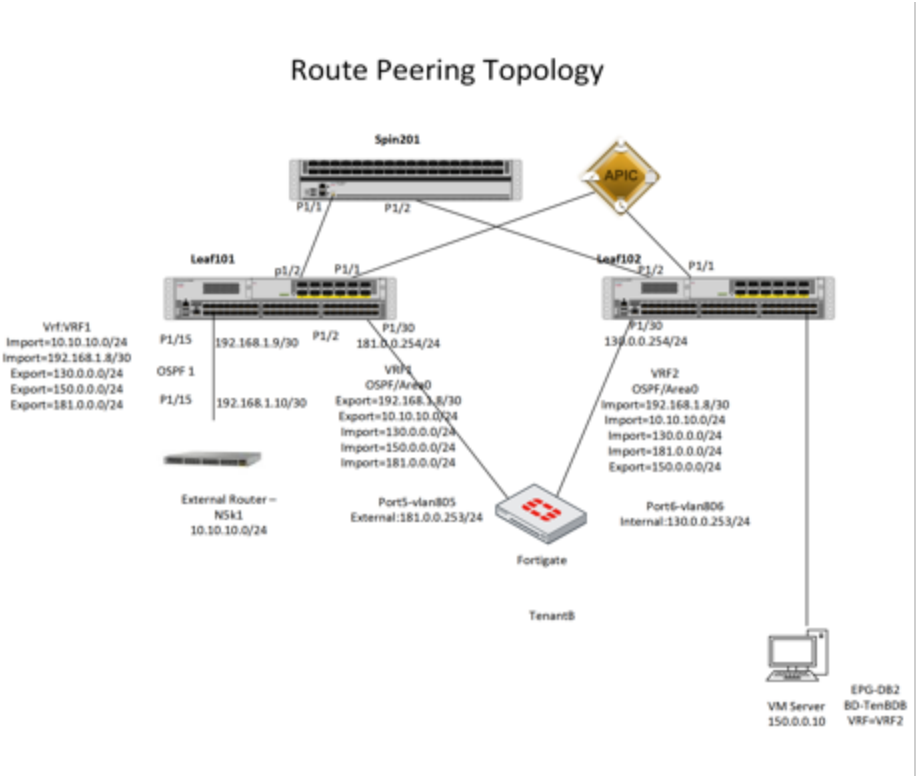


Verify deployed Graph Instance





Deploying Firewall Service for North-to-South traffic with OSPF



Introduction:

This document describes the configuration walkthrough of L4-L7 Service Graph with Route Peering, where the consumer is external to ACI Fabric and the provider is internal to the Cisco ACI Fabric. With route peering feature provided by Cisco APIC, external traffic can reach internal servers through L4-L7 Services.

Prerequisites:

Please pre-configure below configuration before deploying this design:

- Fabric Access Policies creation relating to Vlan Pools, Domain, Attachable Access Entity Profiles, Interface Policies and Switch Policies
- Layer3 Connection Outside of ACI Fabric
- L4-L7 Device Package has imported into Cisco APIC

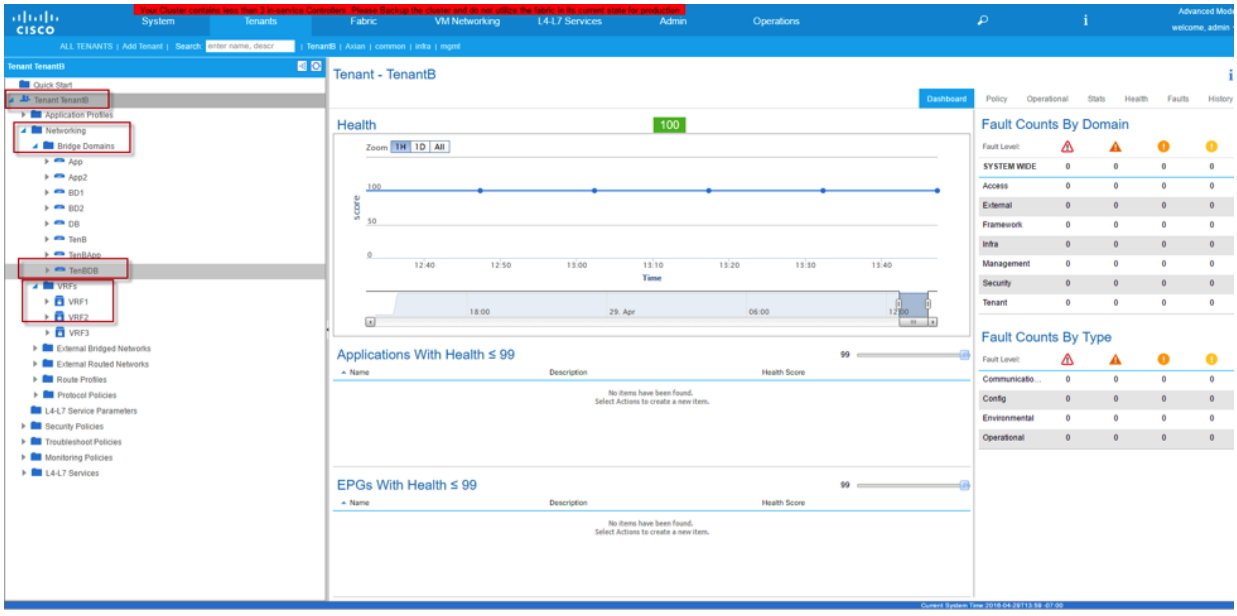
Work Flow:

1. Configure routing configuration on external router that attached to ACI Fabric
2. Create Tenant (TenantB in our example)
3. Create VRFs (VRF1 and VRF2 in our example)
4. Create Bridge Domain and map to VRF2 (TenBDB in our example)

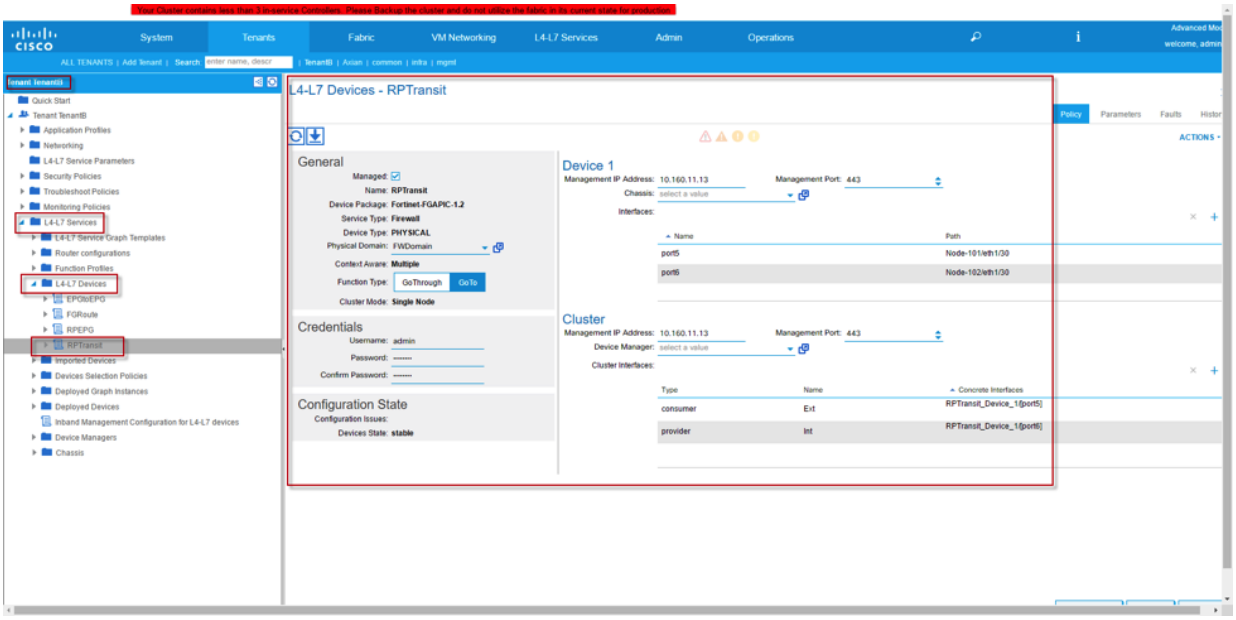
5. Create EPG “EPG-DB2” and map it to Bridge Domain “TenBDB”
6. Create three L3Out EPGs (1 for external Connection, 1 for Firewall External and 1 for Firewall Internal. In our example, we used “N5k-1” for external Connection, “FortigateExternalOut” for Firewall External and “FortigateInternal” for Firewall Internal)
7. Create gateway IP on Bridge Domain (TenBDB) for VM Server
8. Ensure “Unicast Routing” is checked on Bridge Domain “TenBDB”
9. In Bridge Domain “TenBDB”, associate L3Outs to “FortigateInternal”
10. Map VM Server to EPG “EPG-DB2” and configure IP address and gateway ip address (TenBDB ip address)
11. Verify VM Server can ping to gateway IP
12. Create L4-L7 Device
13. Create Functional Profile Group as well as Functional Profile
14. Create Route Profiles
15. Create L4-L7 Service Graph Template
16. Deploy L4-L7 Service Graph

Configuration:

Configure the Bridge Domain TenBDB, VRF1 and VRF2. Associate Bridge Domain TenBDB to VRF2

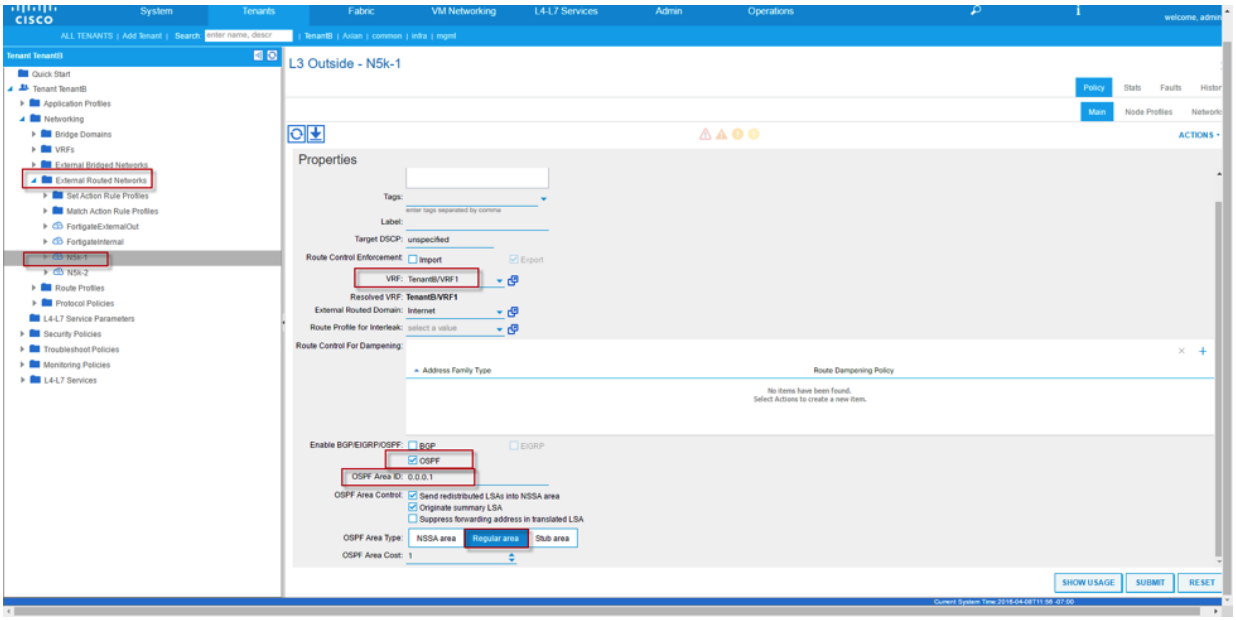


Configure L4-L7 Device for physical Fortigate (GoTo Mode)

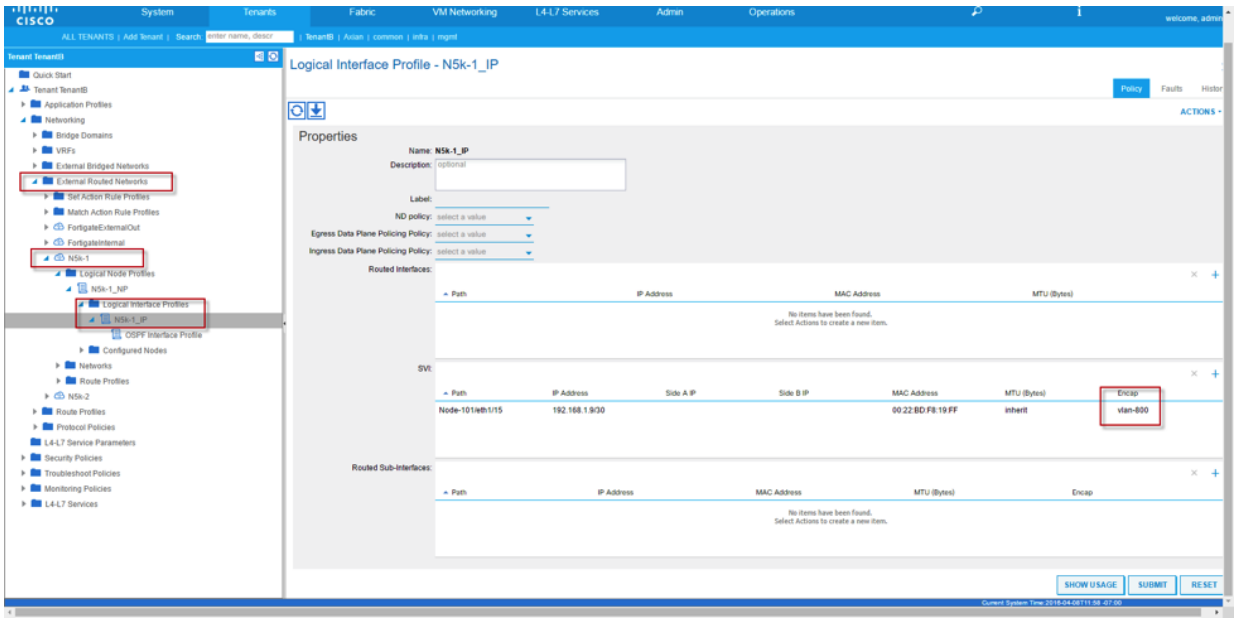


Configure L3Out for N5K-1 and associate to VRF1

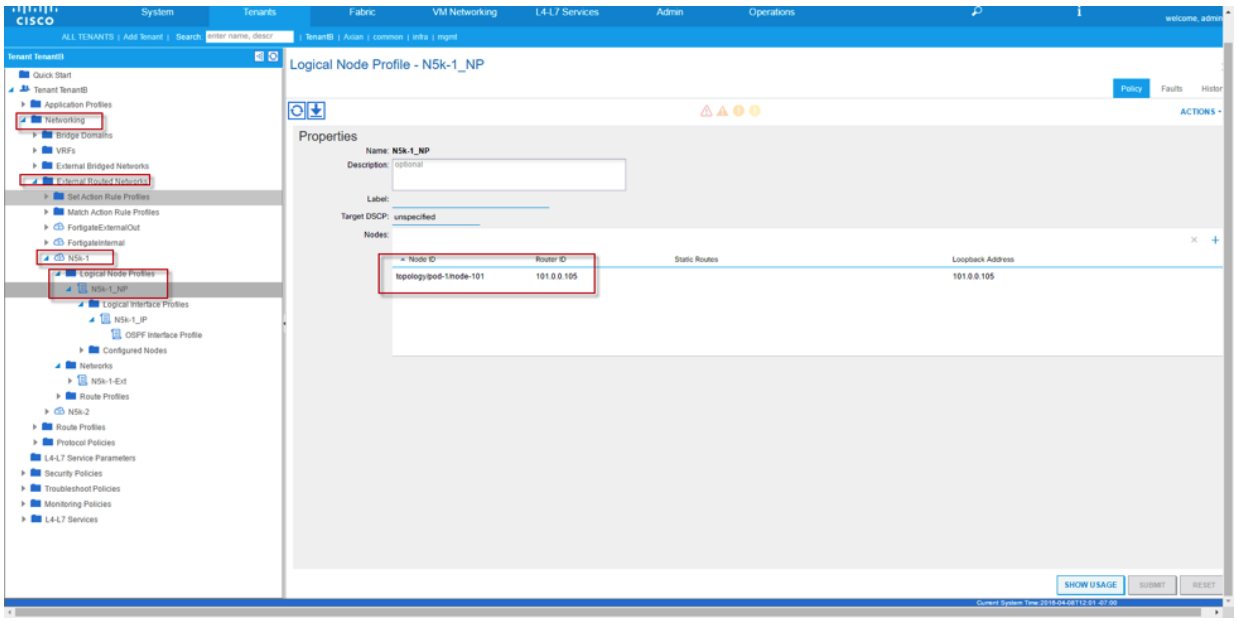
All L3Out Interfaces which are used for Route Peering are required to be configured as a SVI with Vlan Encapsulation accordingly.



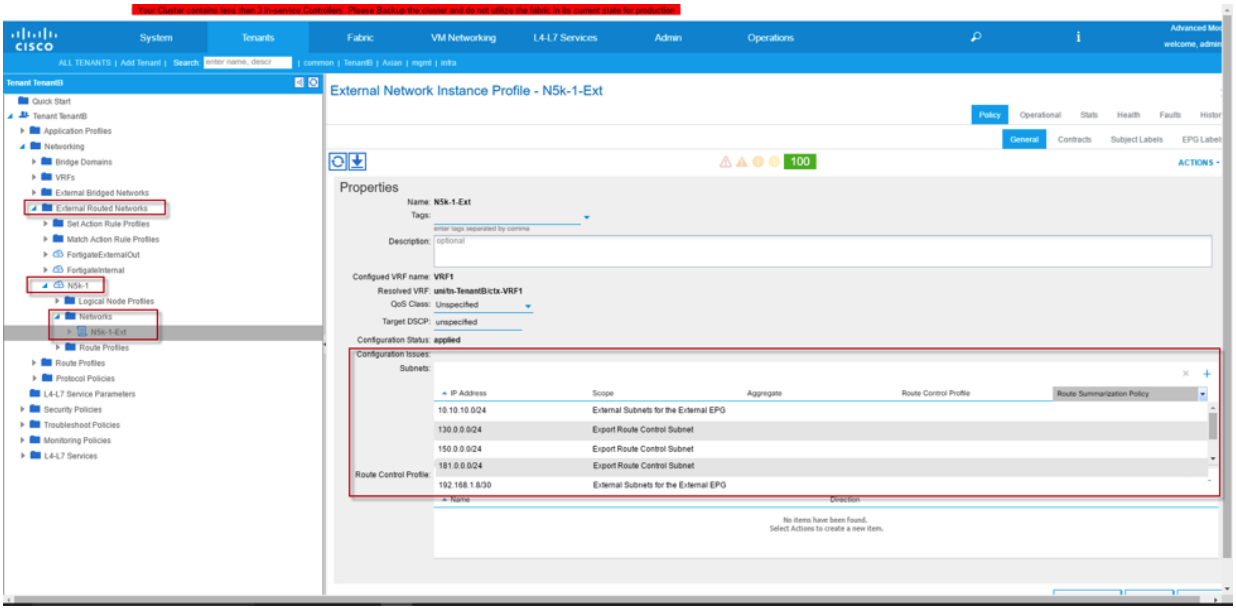
Configure SVI for L3Out N5k-1



Configure Route ID (101.0.0.105 in our example)

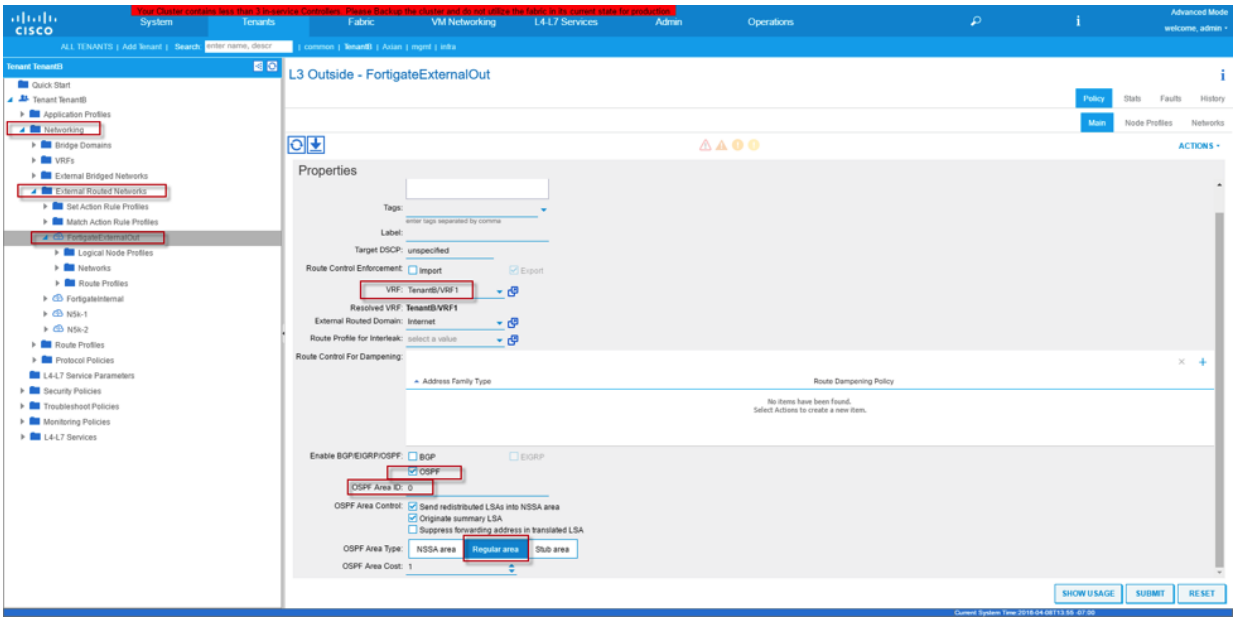


Configure Import/Export Route Control on Subnets for N5k-1 L3Out External EPG

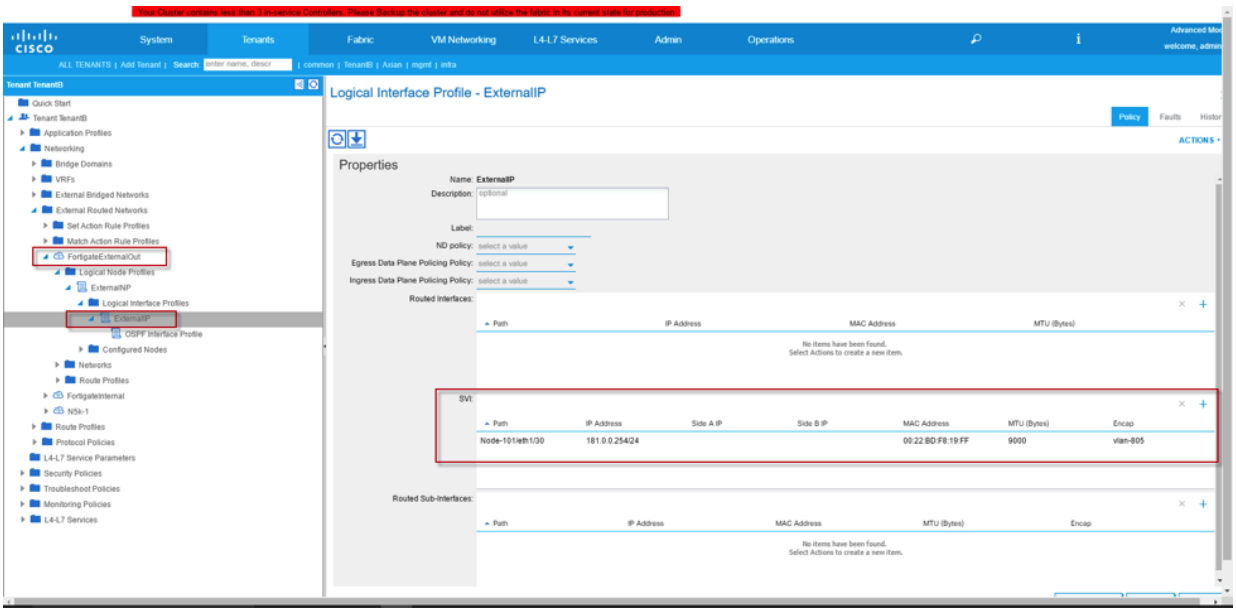


Configure L3Out for Fortigate External Interface (FortigateExternalOut) and associate with VRF1

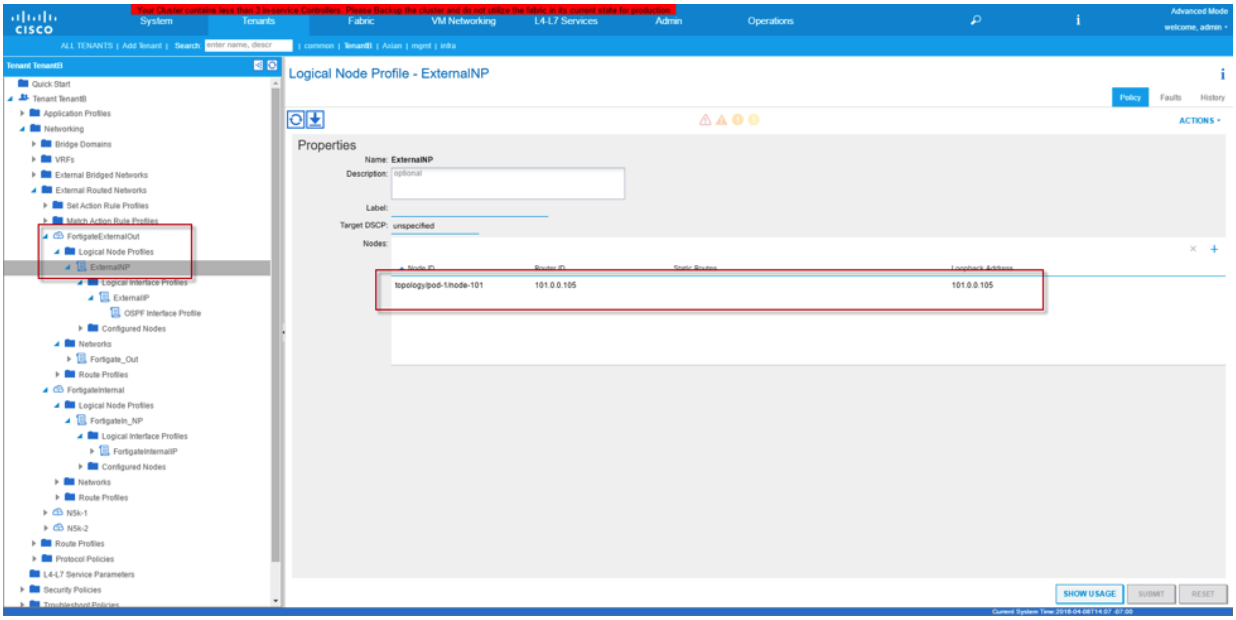
In our example, the route ID here must be the same as above (101.0.0.105), since both L3outs are on the same leaf switch.



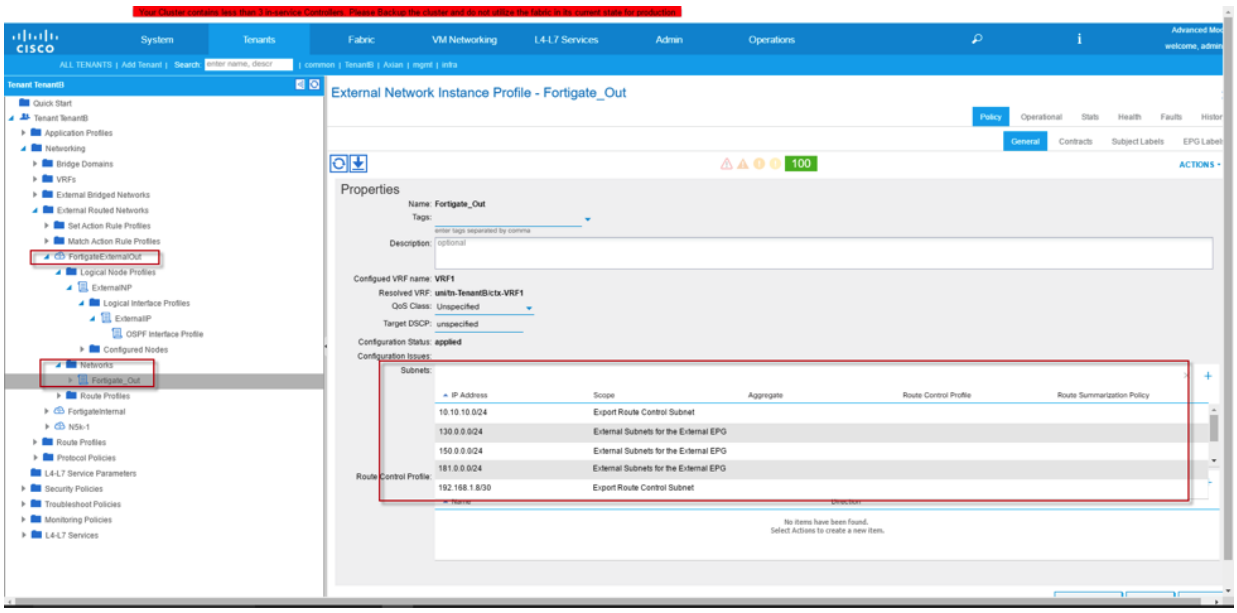
Configure SVI for L3Out Fortigate External out (FortigateExternalOut)



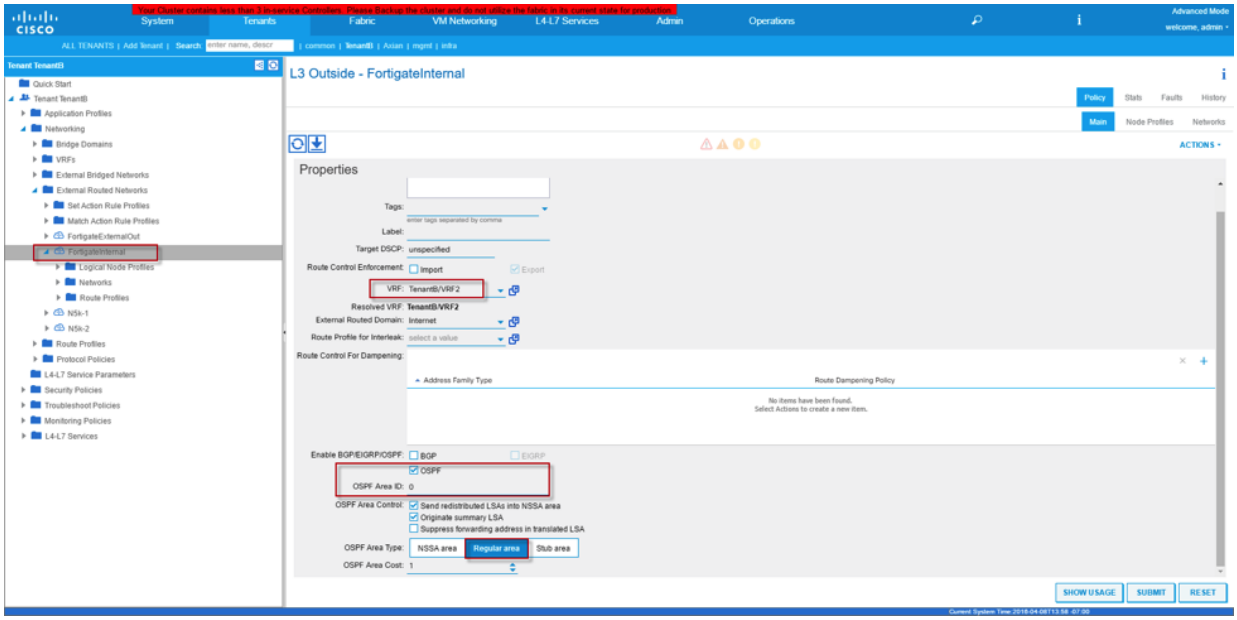
Configure Route ID for L3Out Fortigate External Out (FortigateExternalOut)



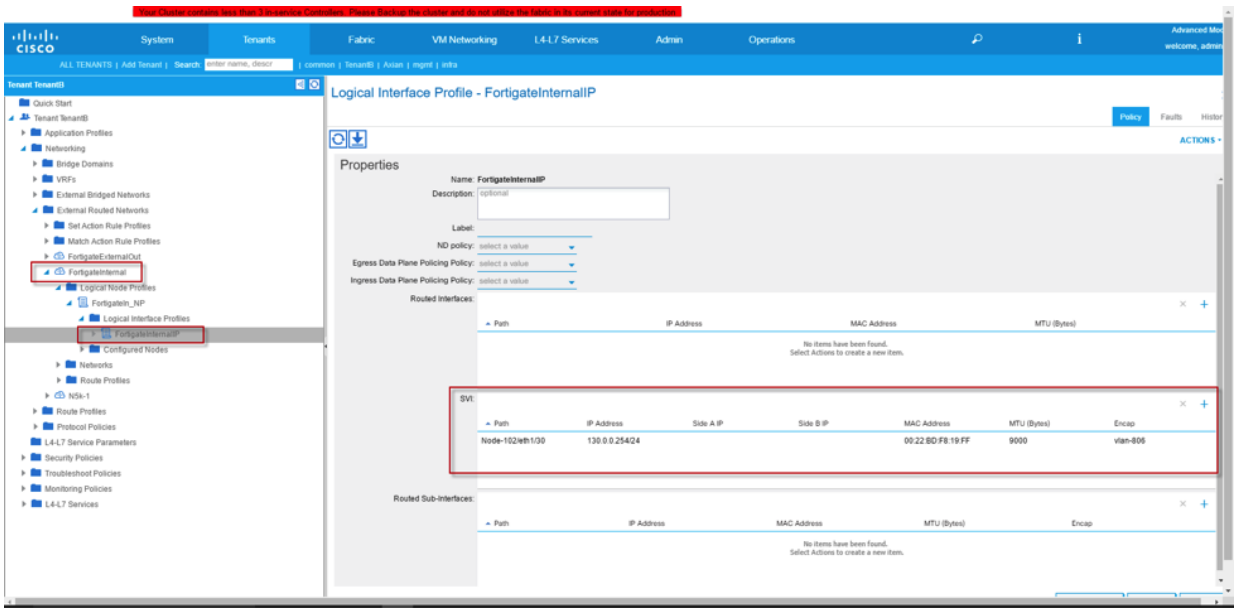
Configure Import/Export Route Control on Subnets for Fortigate External out



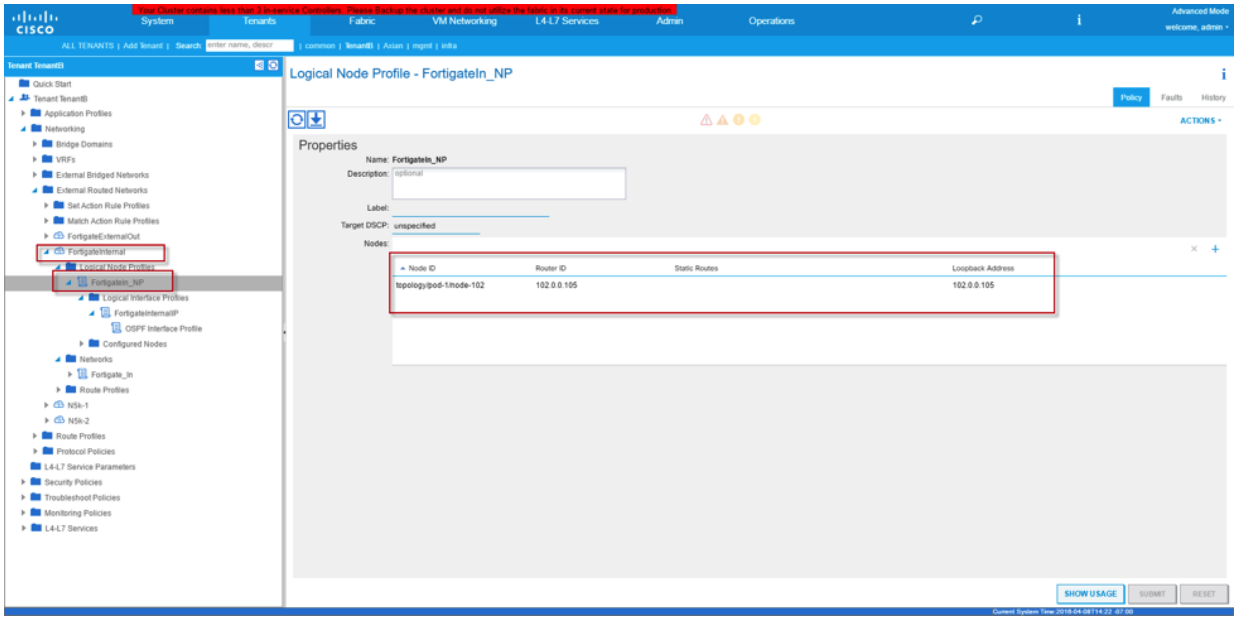
Configure L3Out for Fortigate Internal (FortigateInternal) and associate with VRF2



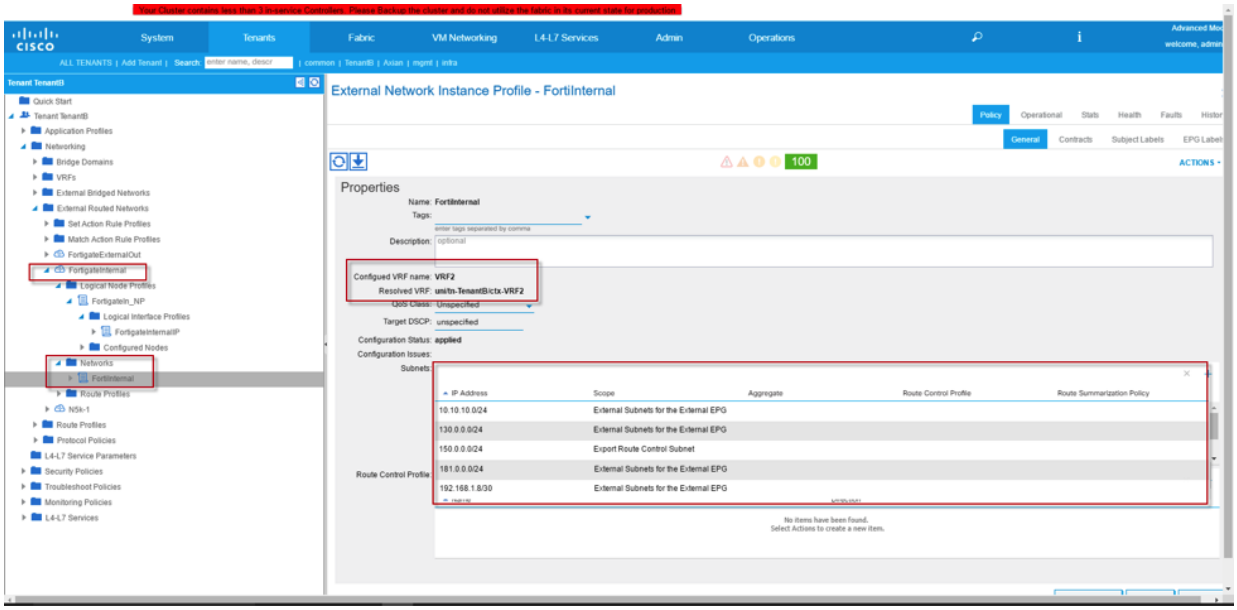
Configure SVI for L3Out Fortigate Internal (FortigateInternal)



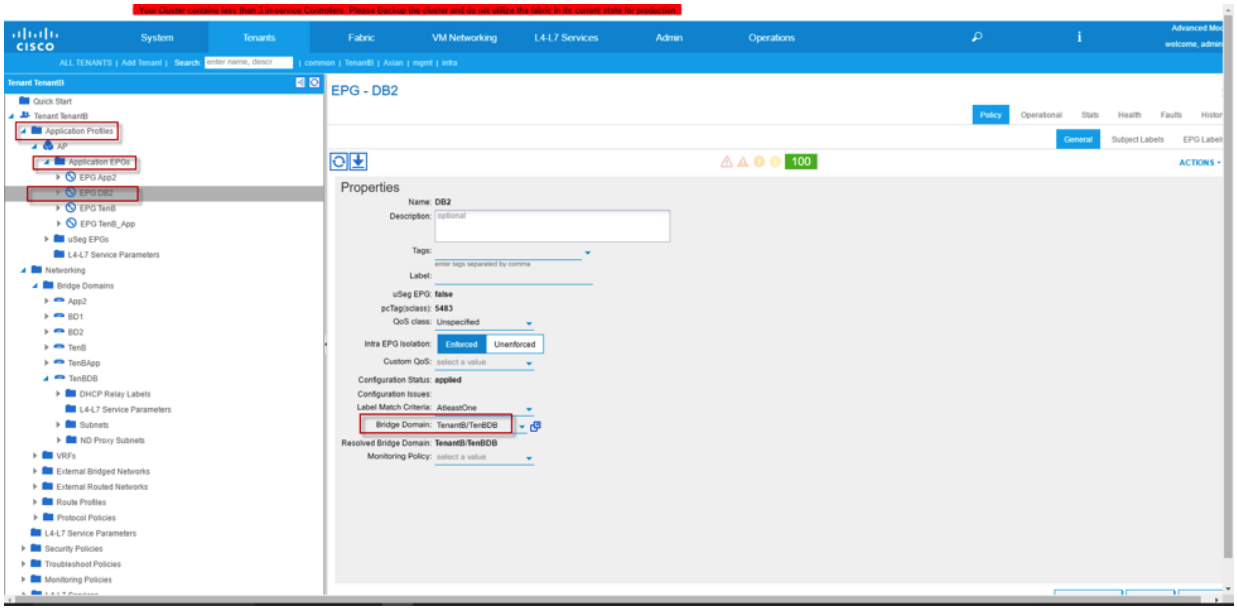
Configure Route ID for L3Out Fortigate Internal (FortigateInternal)

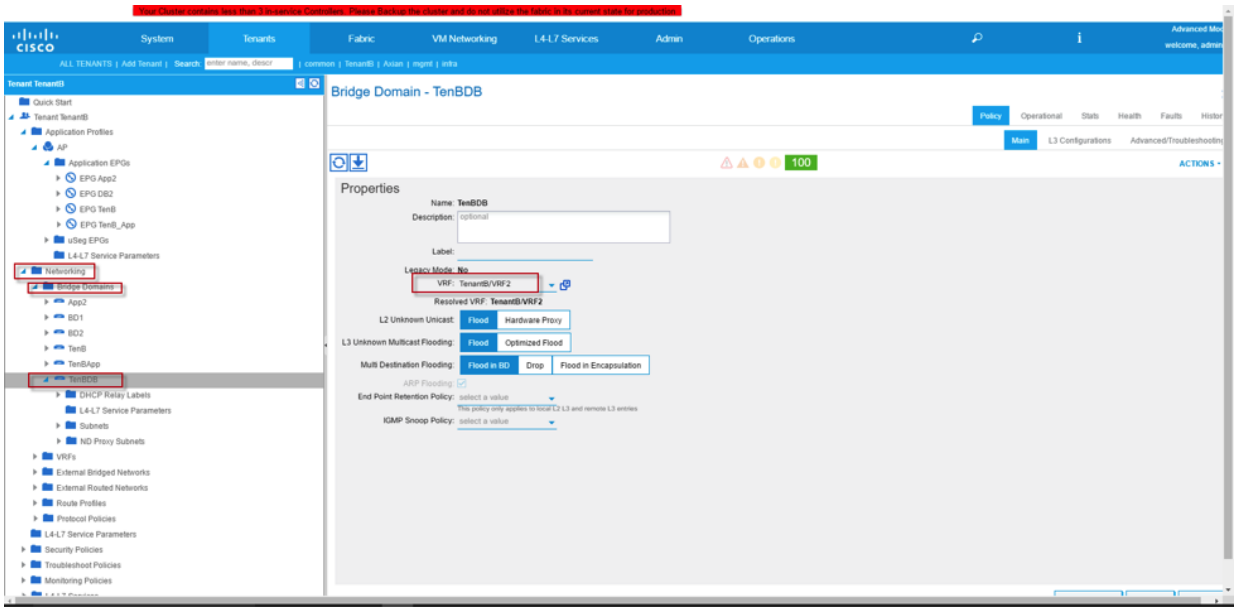


Configure Import/Export Route Control on Subnet for L3Out Fortigate Internal (FortigateInternal)

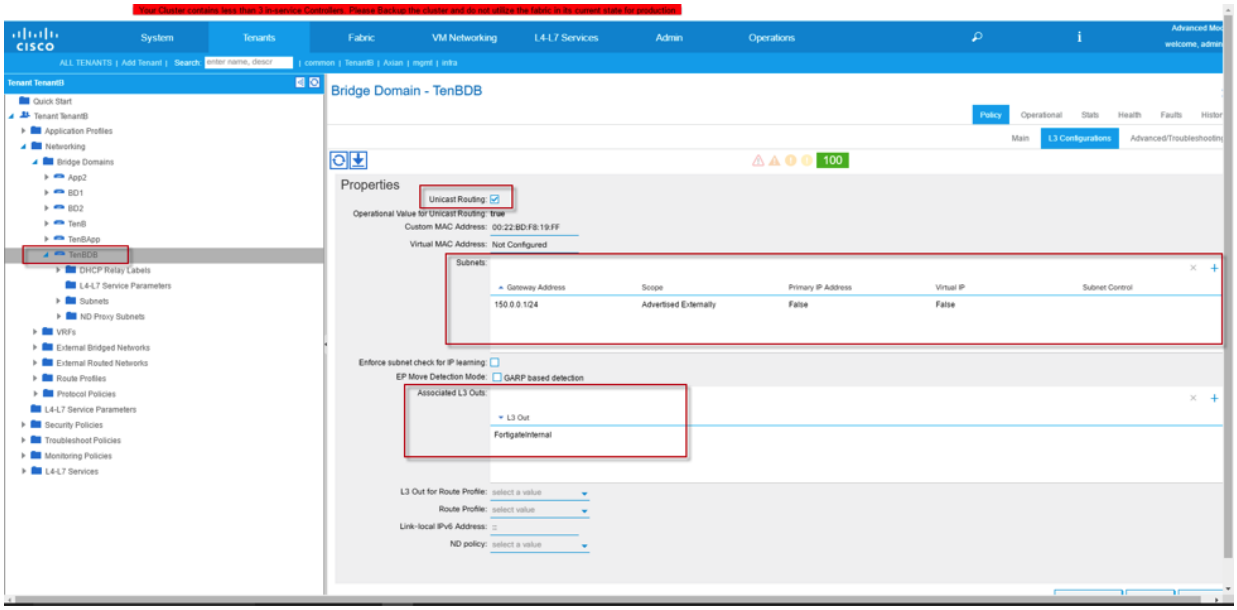


Associate EPG “DB2” to Bridge Domain “TenBDB” and attach Bridge Domain to VRF2

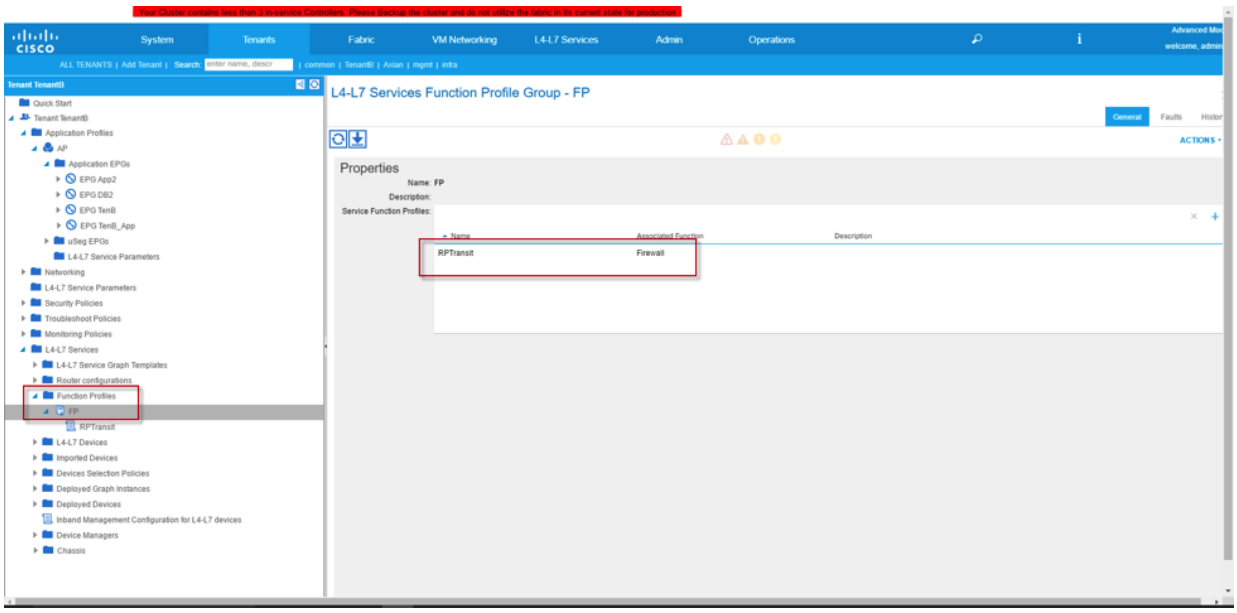


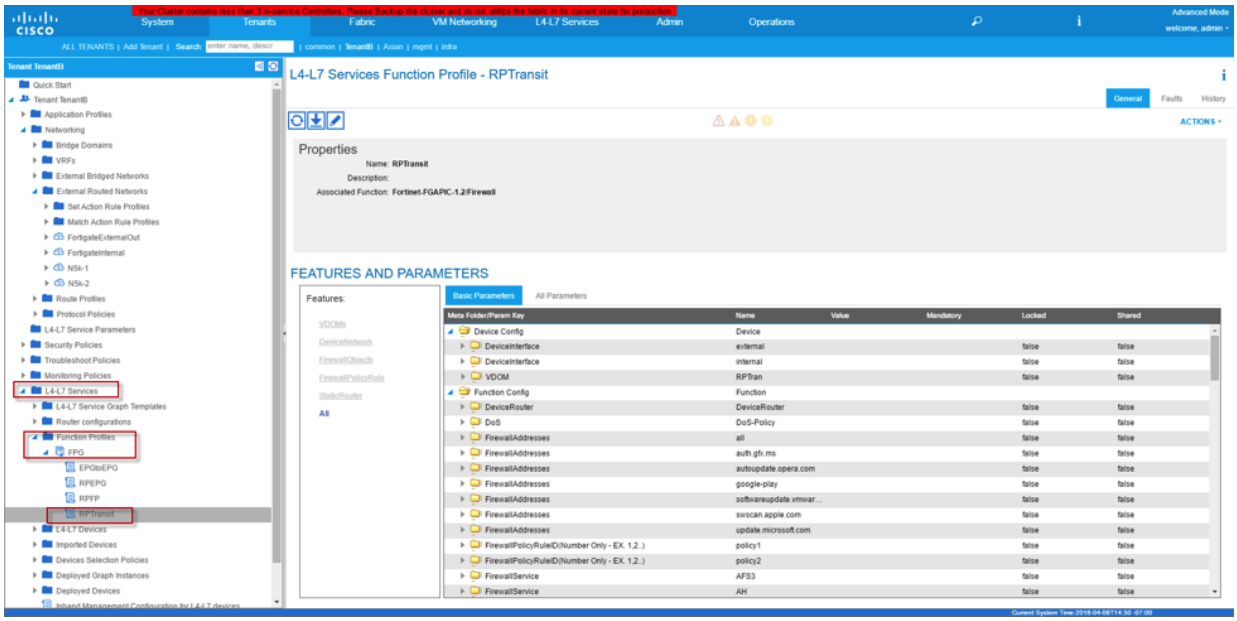


Configure Bridge Domain with Unicast Routing, assign SVI and associate L3Outs to “FortigateInternal”

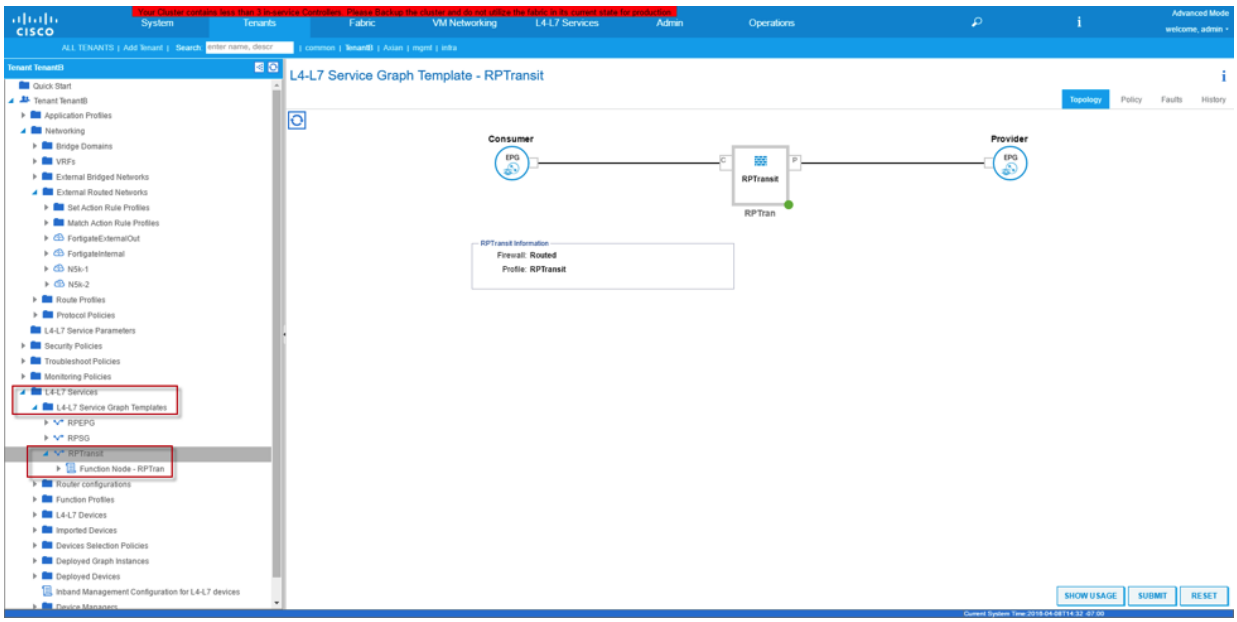


Create Functional Profile Group and Functional Profile from existing template

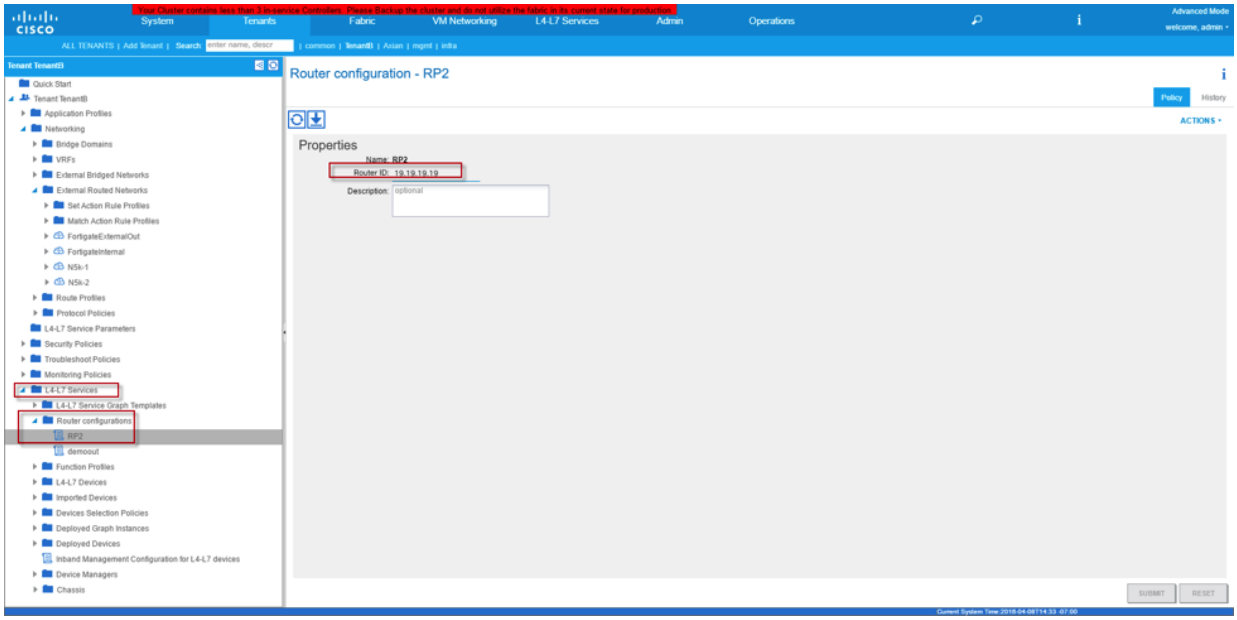




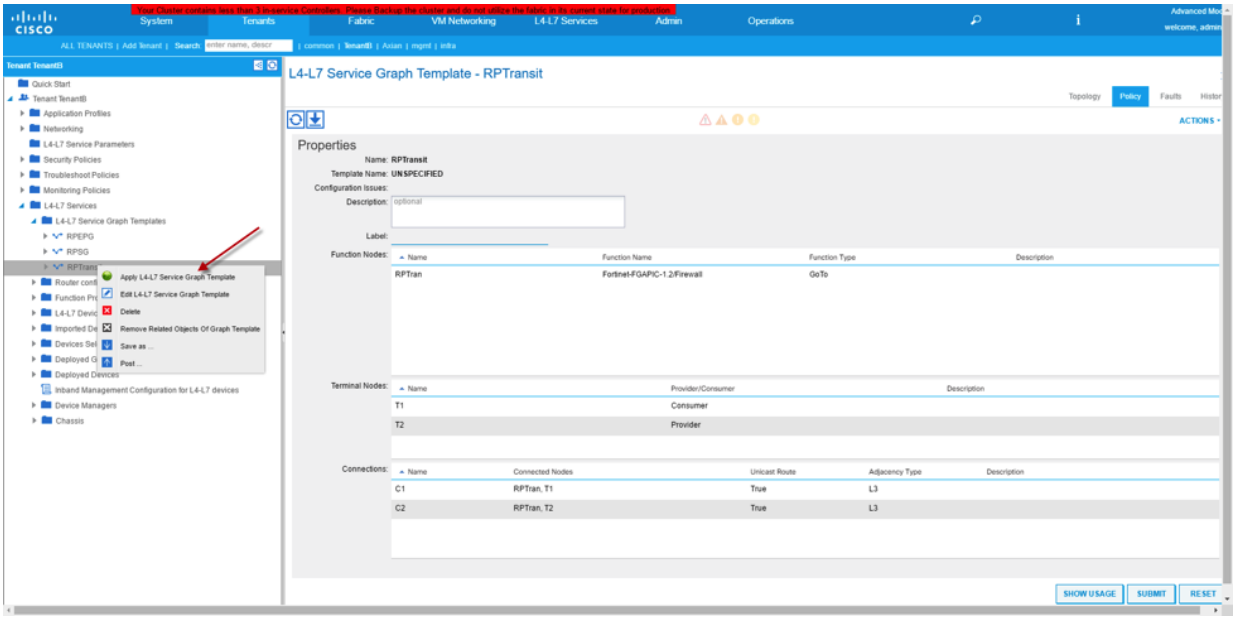
Create Service Graph template



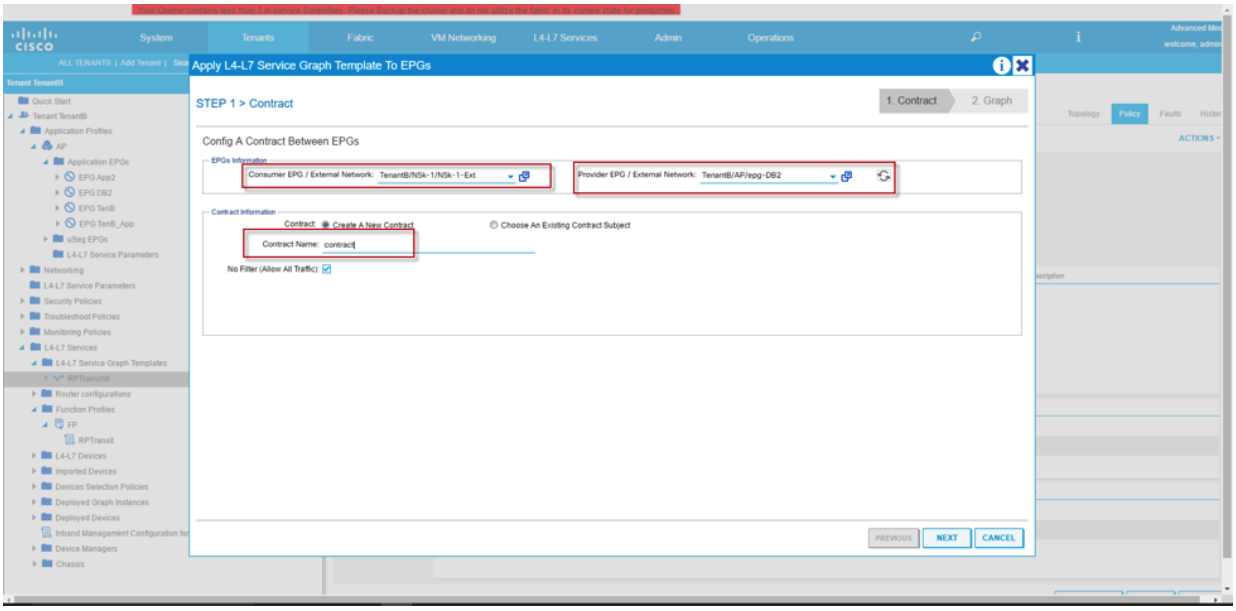
Create Router ID that will be used on the Service Appliance (Fortigate)



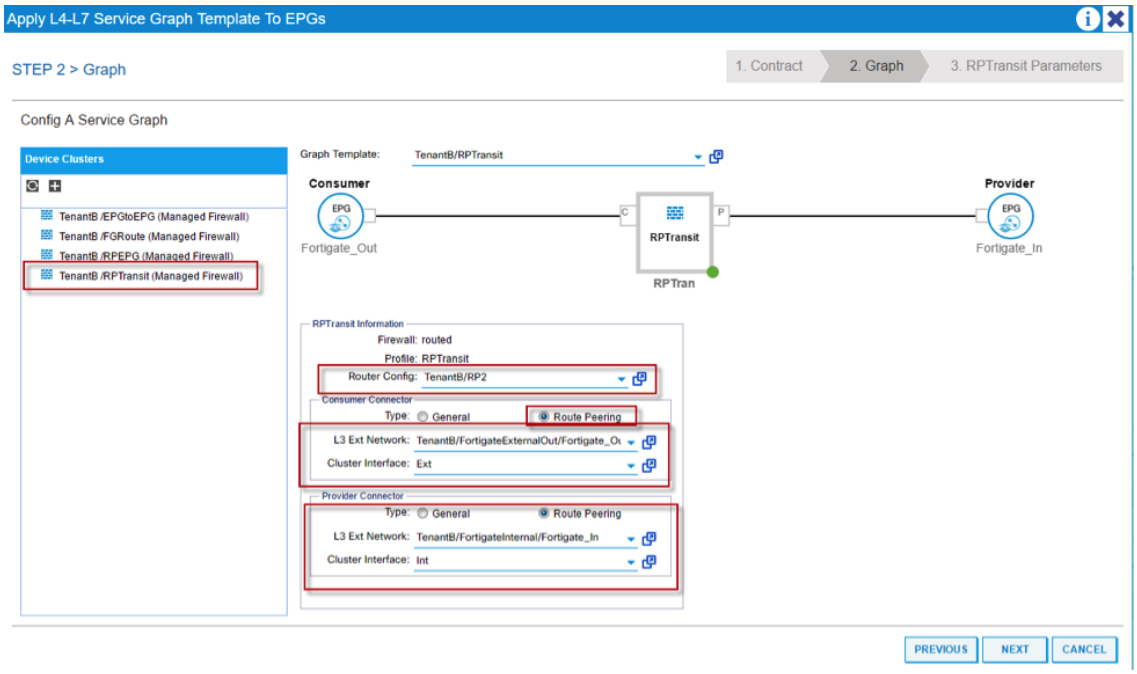
Deploy Service Graph



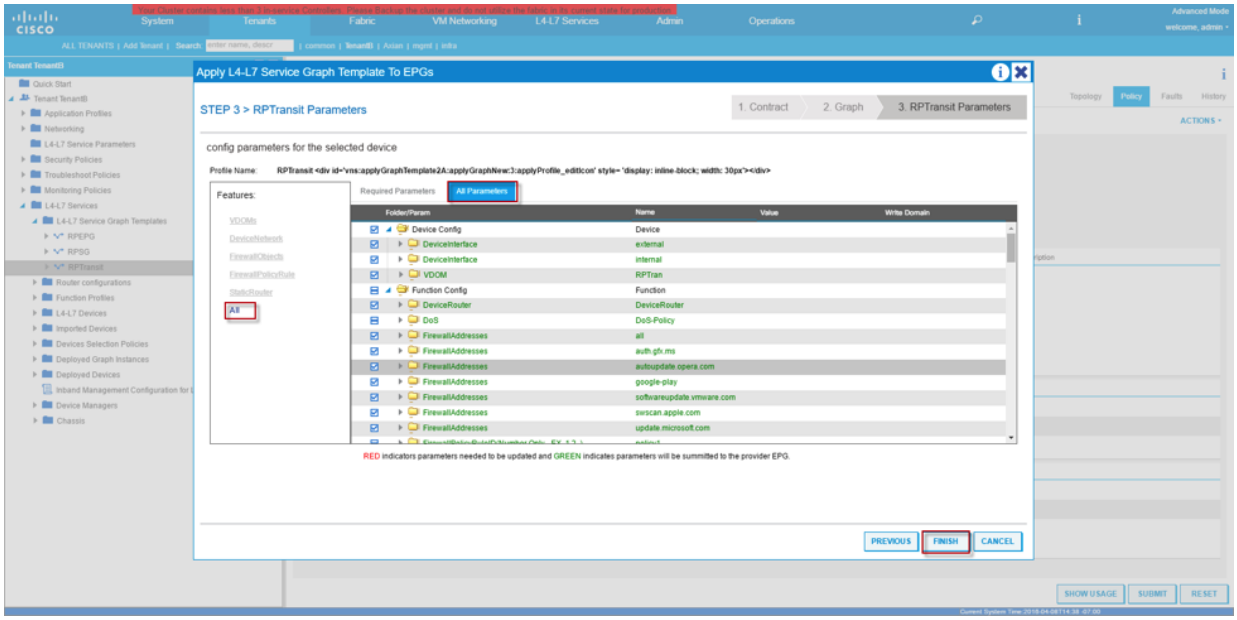
Consumer will be L3Outs facing external router. Provider is the internal EPG. In our case will be N5k-1 and DB2 respectively.



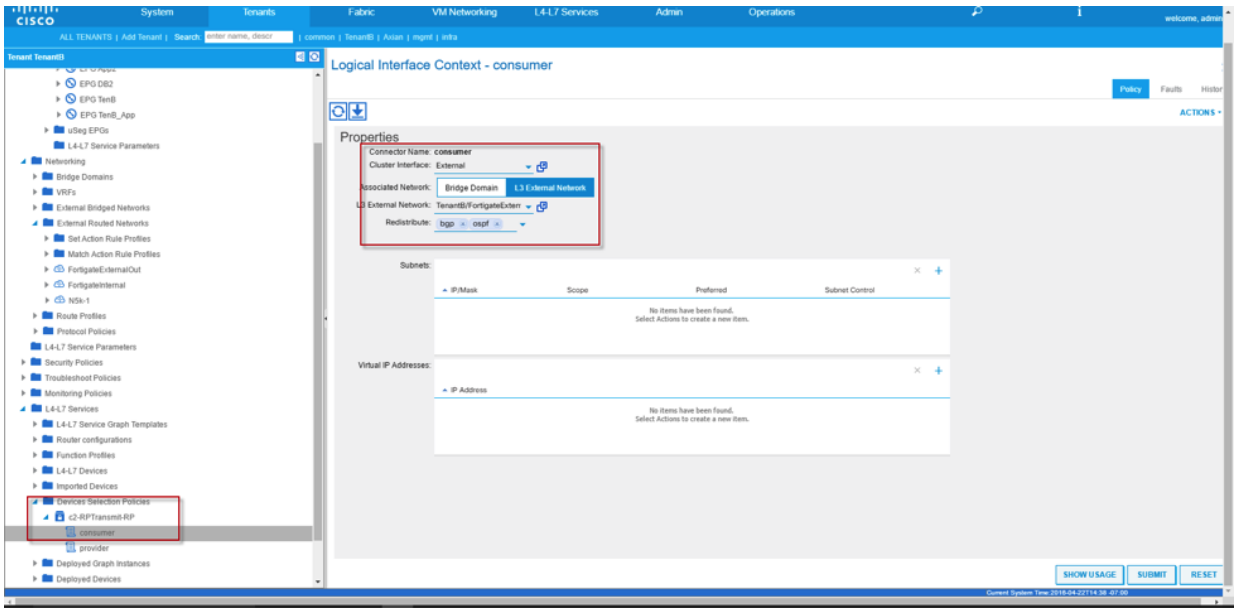
Route peering needs to be select for Internal and external connections. In our example, we used “FortigateExternalOut” and FortigateInternal” as External and Internal selections respectively.

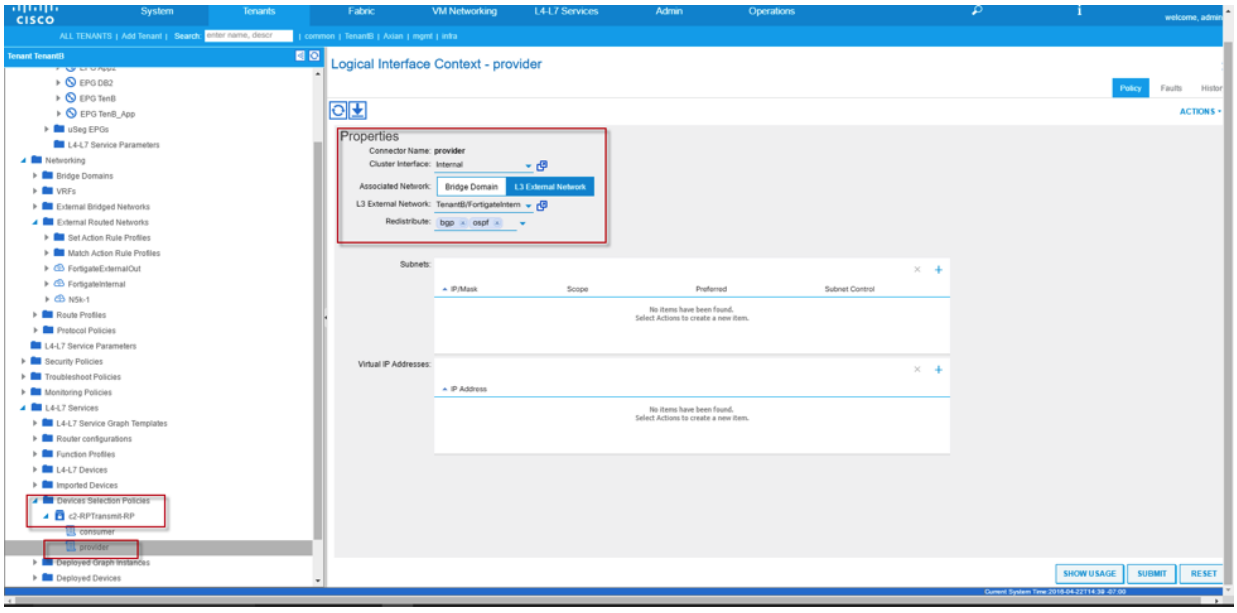


Last minute check to make sure configuration is good before hit “Finish” button

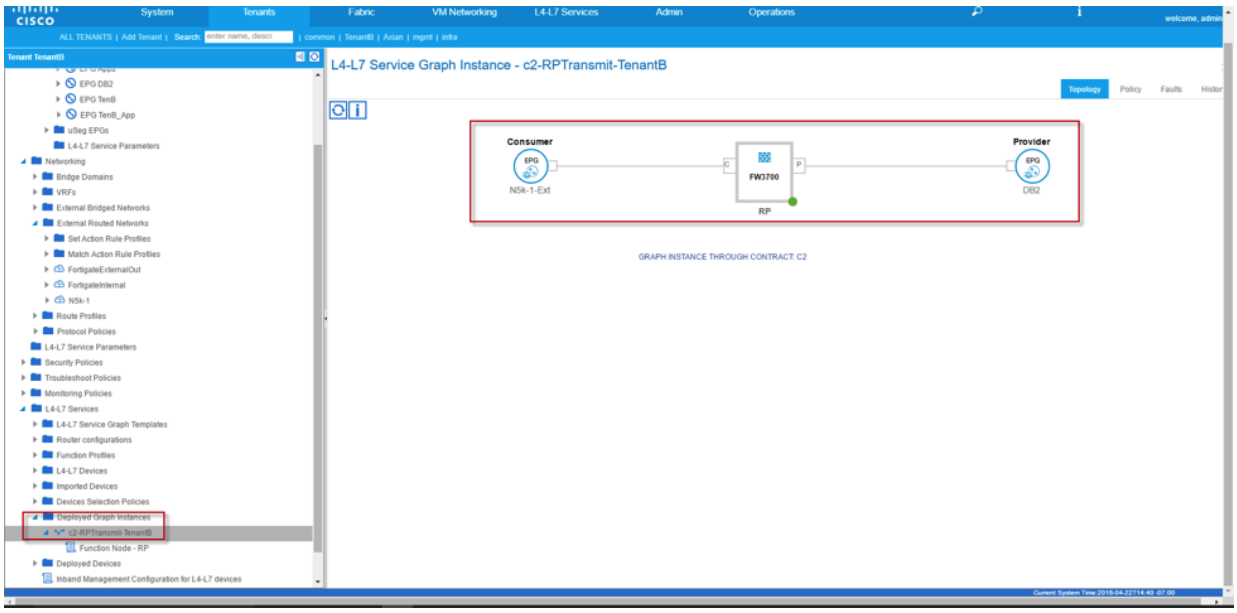


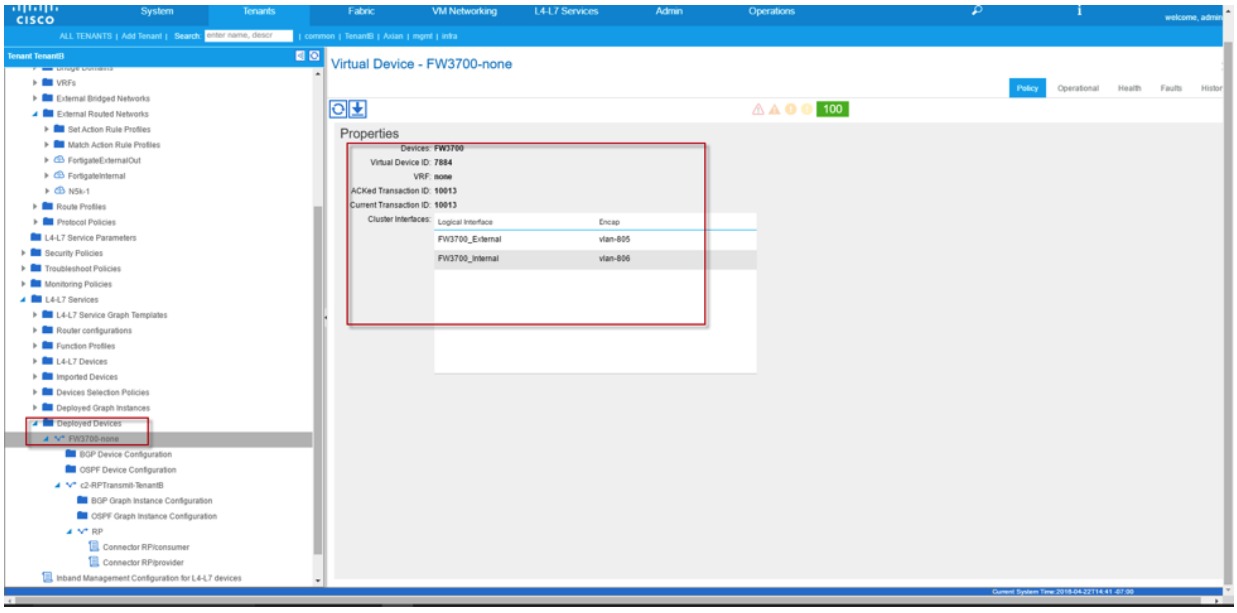
Check the status and verify Device Selection Policy





Verify deployed Graph Instance





Deploying Firewall service with Fortigate-VM and VmWare

Pre-requisite

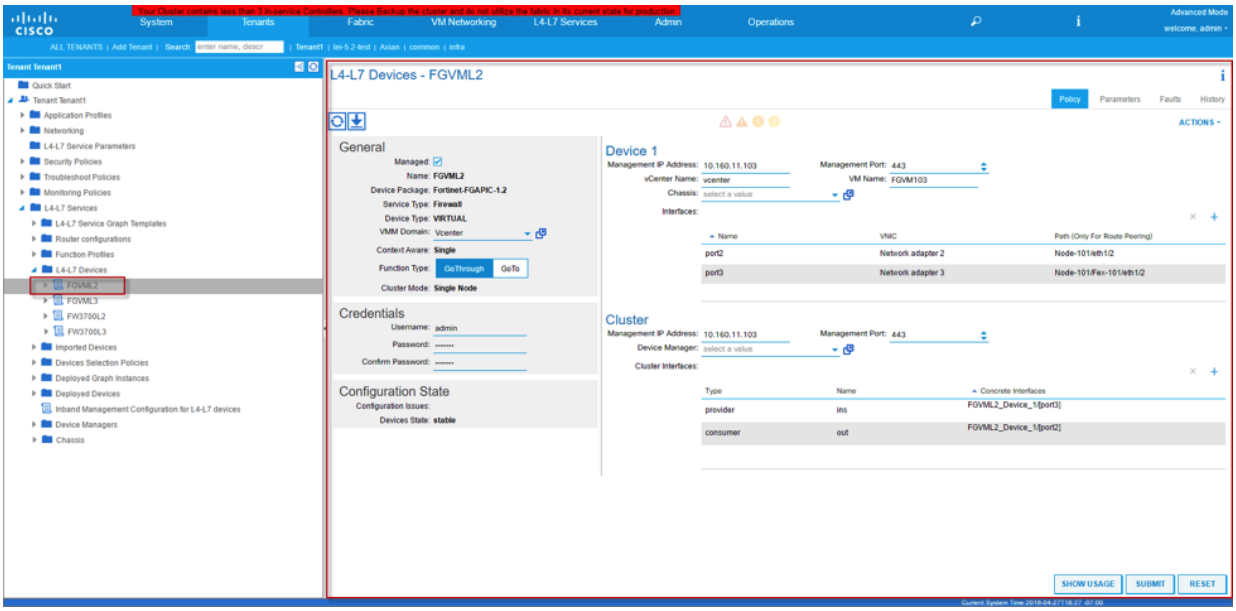
- Fabric Access Policies creation relating to Vlan Pools, Domain, Attachable Access Entity Profiles, Interface Policies and Switch policies
- Create Tenant, VRF, 2 Bridge Domains, 2 EPGs
- Associate2 Bridge Domains to VRF
- Associate 2 EPGs to the 2 Bridge Domains
- Layer4-7 Device Package has imported into Cisco APIC

Work Flow:

1. Create Go-Through mode Fortigate VM Devices on Cisco APIC
2. Create Functional Profile
3. Create Service Graph Template
4. Deploy Service Graph

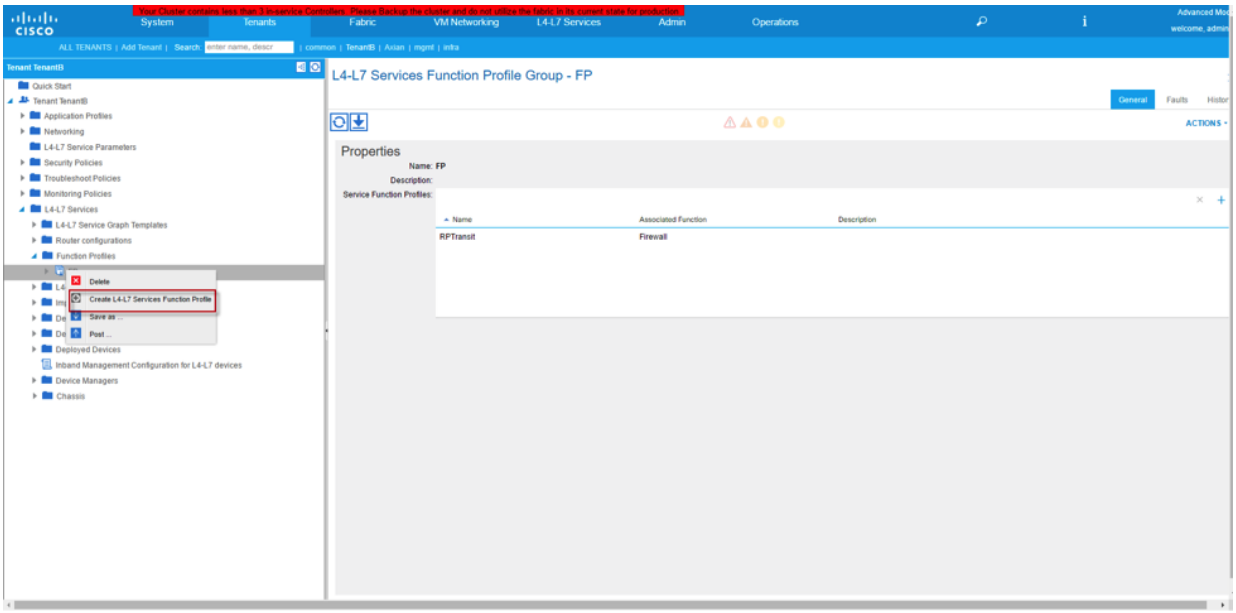
Configuration

Create Layer 4-L7 Device on Cisco APIC



Create Functional Profile

Functional Profile defines the template for the Service(s) that is going to deploy such as L4-L7 Device Interface IP addresses, Rule ID, Object Addresses, Policy Rules, Source/Destination Ports…etc.



Functional Profile Objects Explanation under “Features”

Device Network:

Contained External and Internal Interfaces that will be programmed onto Fortigate VDOM. This is the interfaces (typically external and internal) that will be associated to the VDOM.

Similar to above notes, for Go-To Mode, please modify the IP address field otherwise leave the default for Go-Through Mode.

Firewall Objects:

This field allows user to customize Firewall Addresses, Service and scheduling.

Firewall Policy Rule:

This field encompassed the creation of Firewall policy that will be program onto Fortigate. Security Profile and Logging Options are also configured here.

Static Router:

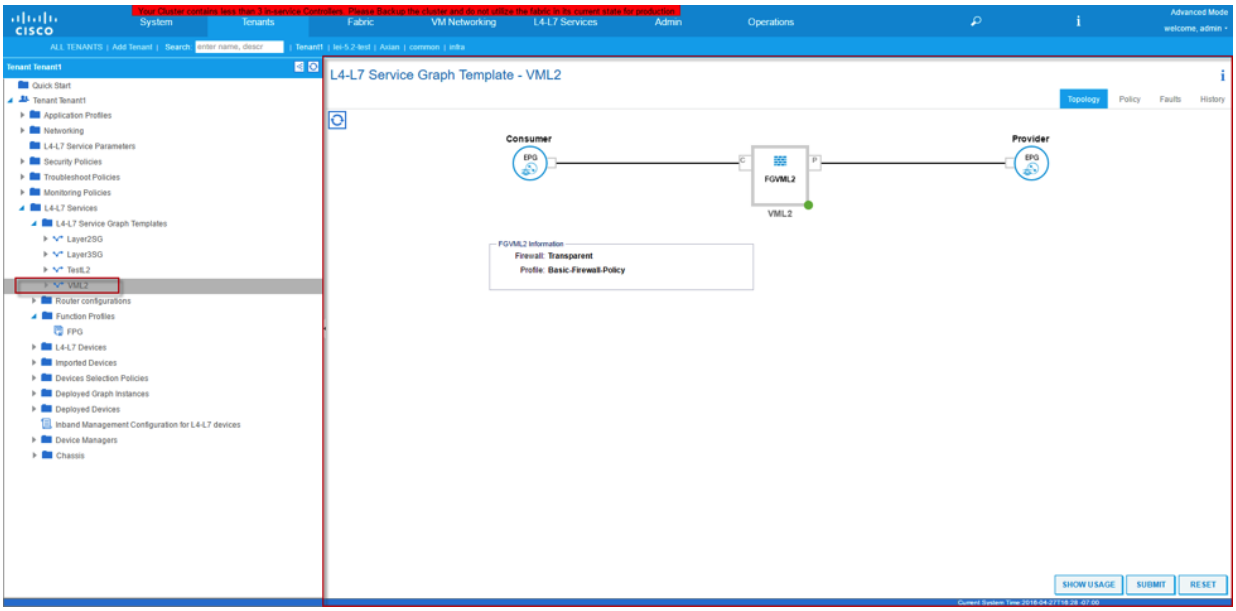
Allow user to configure static route that will be used on Fortigate.

All:

This field listed all the parameters stated above plus DDOS configuration.

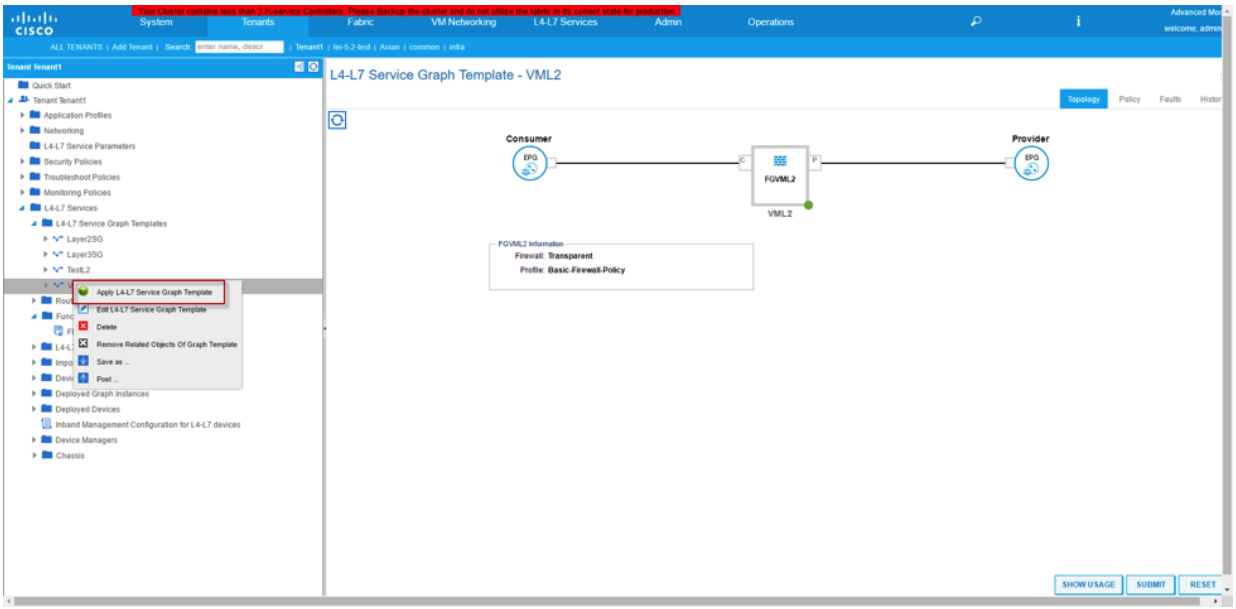
Create Service Graph

Service Graph template is used to tightly coupled the Functional Profile or Firewall configuration and combine with the Firewall device we defined at earlier steps.

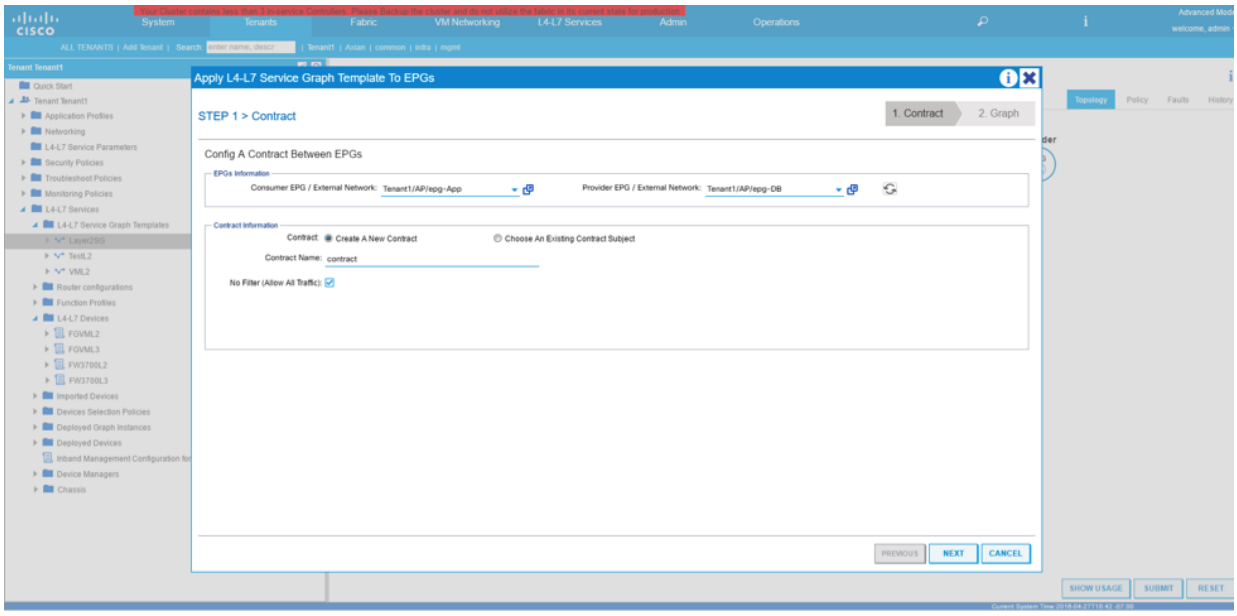


Deploy Service Graph

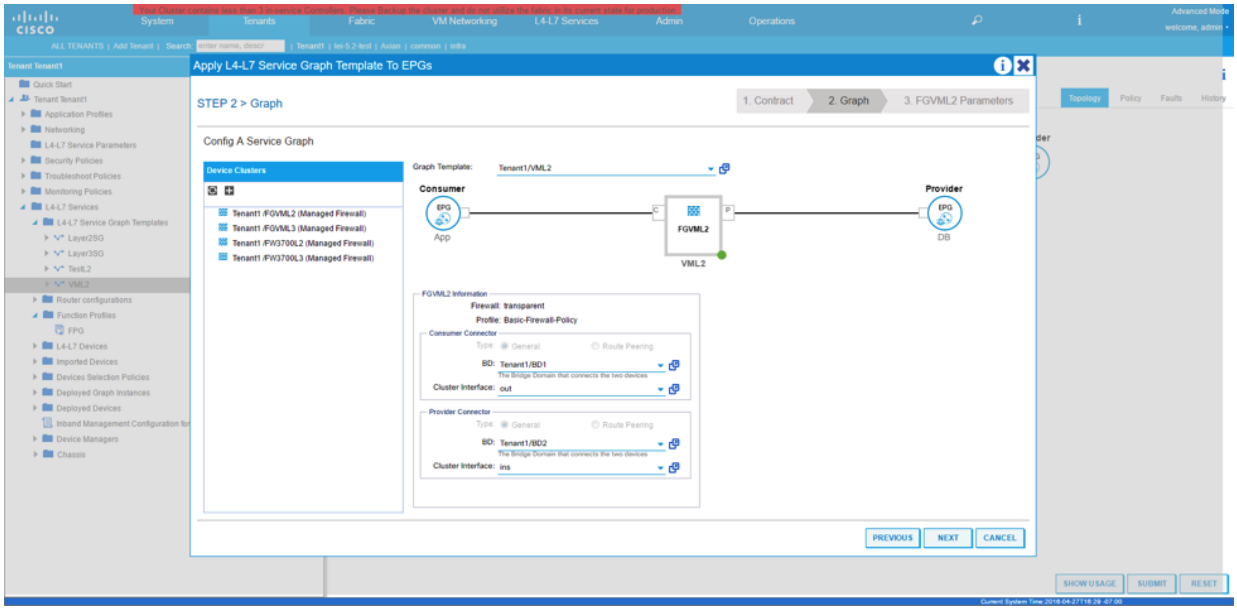
Once we combined the Firewall configuration and associated device together, we are ready to deploy the service Graph to create a VDOM.



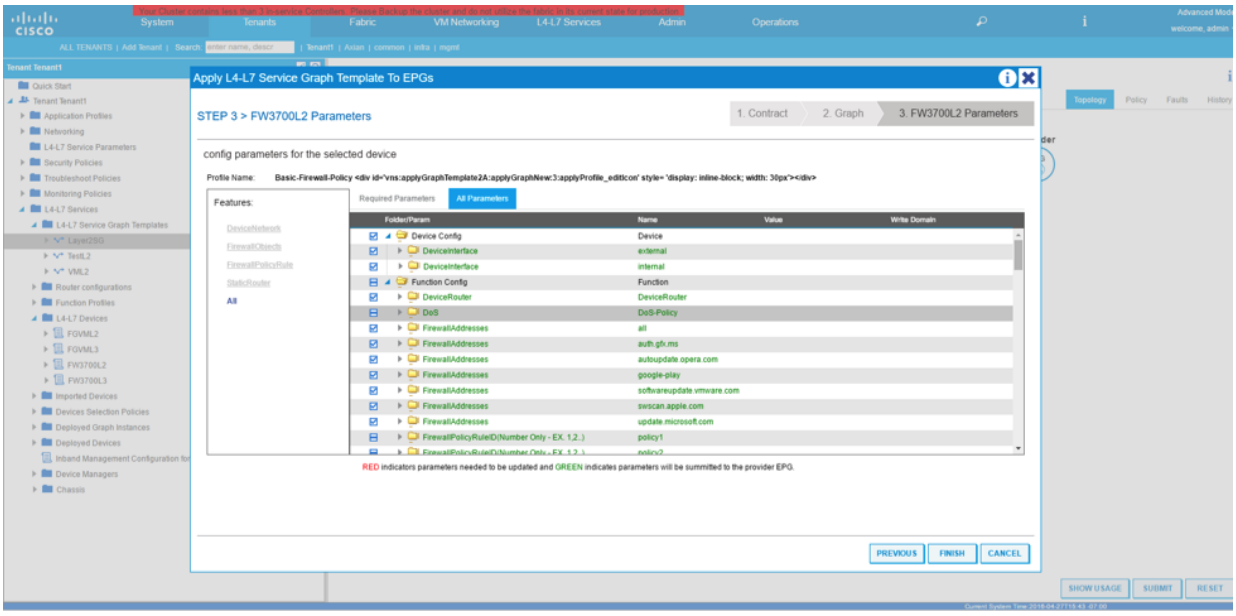
On next screen select the Consumer and provider EPGs and assign a contract name or select a pre-define contract.



Next screen select the logical interfaces defined during the creation of Layer4-7 Device.



Next screen to the last minute check to ensure everything is accordingly before deploy. If ok, then hit the submit button.


Apply L4-L7 Service Graph Template To EPGs
STEP 3 > FW3700L2 Parameters
1. Contract
2. Graph
3. FW3700L2 Parameters
config parameters for the selected device
Profile Name:
Features:
Required Parameters
All Parameters
Folder/Param
Name
Value
Write Domain
Device Config
DeviceInterface
external
DeviceInterface
internal
Function Config
DeviceRouter
DoS
DoS-Policy
FirewallAddresses
all
FirewallAddresses
auth.gfx.ms
FirewallAddresses
autoupdate.opera.com
FirewallAddresses
google-play
FirewallAddresses
softwareupdate.vmware.com
FirewallAddresses
swscan.apple.com
FirewallAddresses
update.microsoft.com
FirewallPolicyRuleID(Number Only - EX. 1,2..)
policy1
RED indicators parameters needed to be updated and GREEN indicates parameters will be summitted to the provider EPG.
PREVIOUS
FINISH
CANCEL
SHOW USAGE
SUBMIT
RESET

Deploy the firewall device shared by multiple service graphs

Pre-requisite

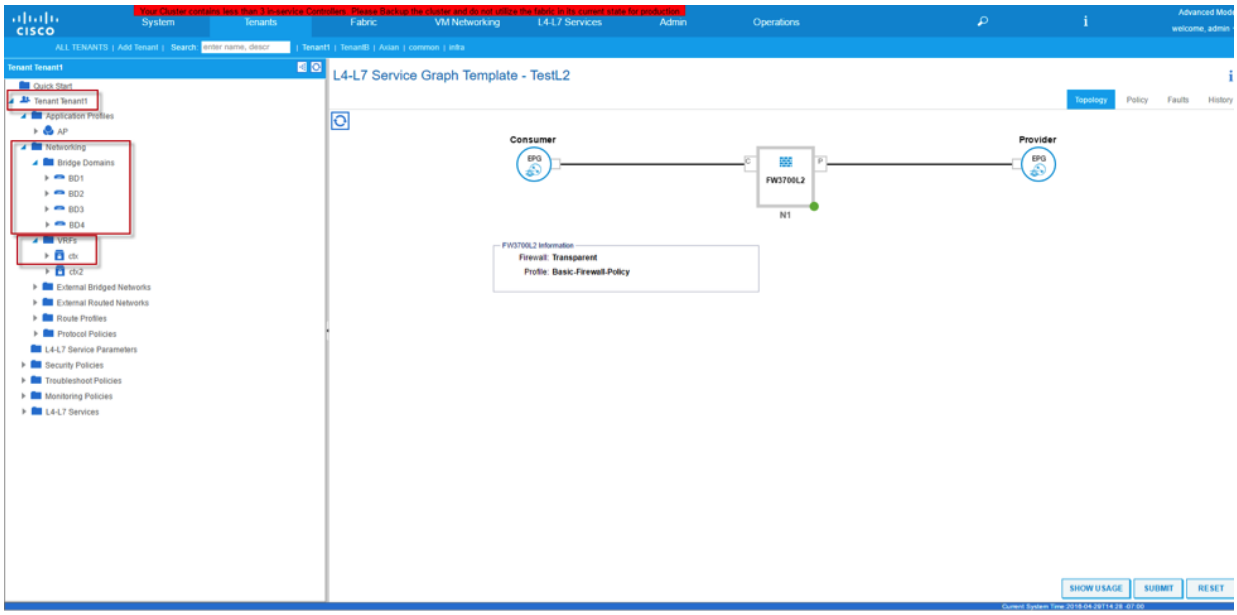
- Fabric Access Policies creation relating to Vlan Pools, Domain, Attachable Access Entity Profiles, Interface Policies and Switch policies
- Layer4-7 Device Package has imported into Cisco APIC

Work Flow:

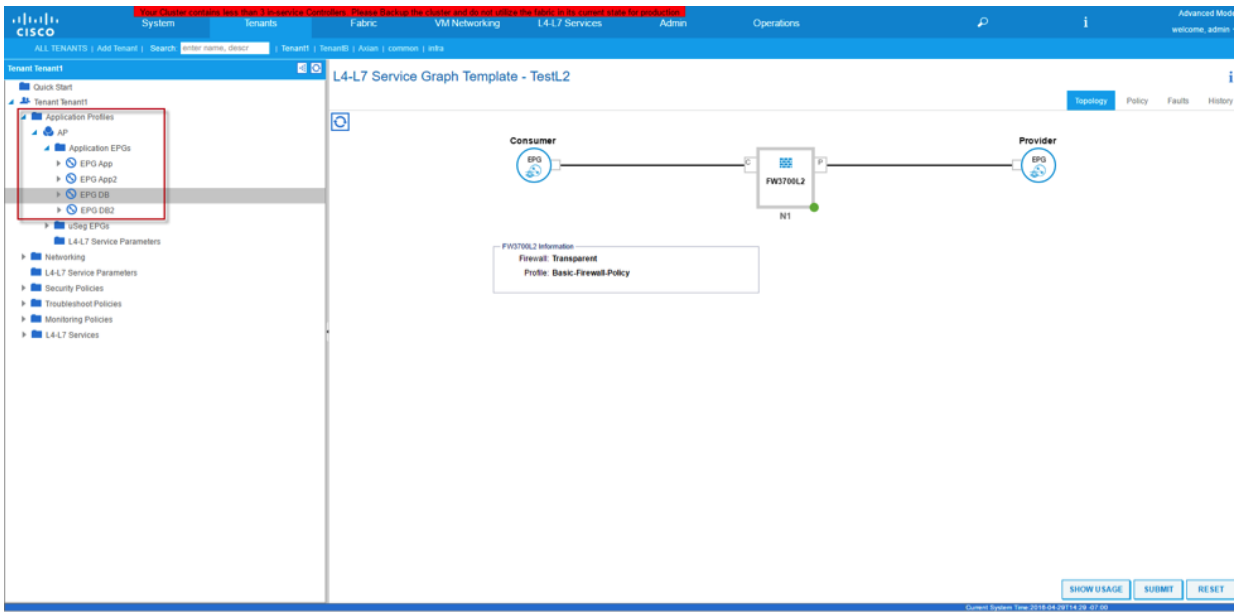
1. Create Tenant (“Tenant1” in our example)
2. Create VRF (“ctx” in our example)
3. Create 4 Bridge Domains (“BD1”, “BD2”, “BD3” and “BD4” in our example)
4. Associate Bridge Domains to VRF
5. Create 4 EPGs (“App” , “App2”, “DB”, “DB2” in our example)
6. Associate EPGs to Bridge Domains (EPG “App”, “App2”, “DB” and “DB2” are mapped to Bridge Domain “BD1”, “BD2”, “BD3” and “BD4” respectively in our example)
7. Create Go-Through mode Device on Cisco APIC and define 4 logical interfaces
8. Create Functional Profile
9. Create 2 Service Graph Templates
10. Deploy Service Graph 2 times on the same device but with different EPG pairs

Configuration

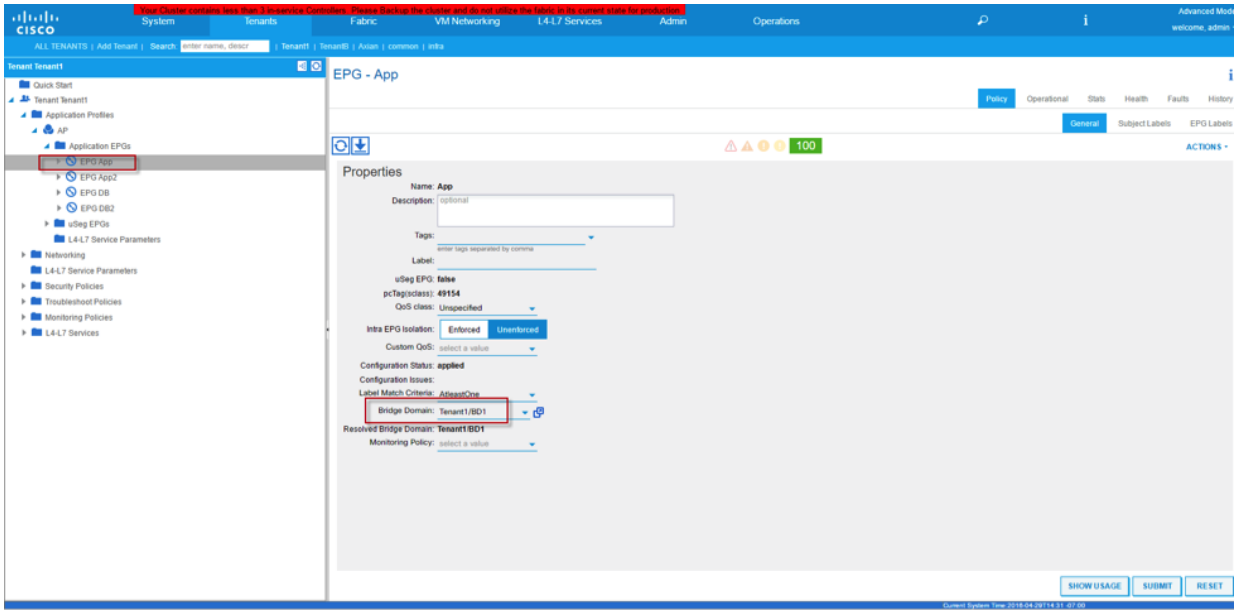
Create Tenant, VRF and 4 Bridge Domains on Cisco APIC

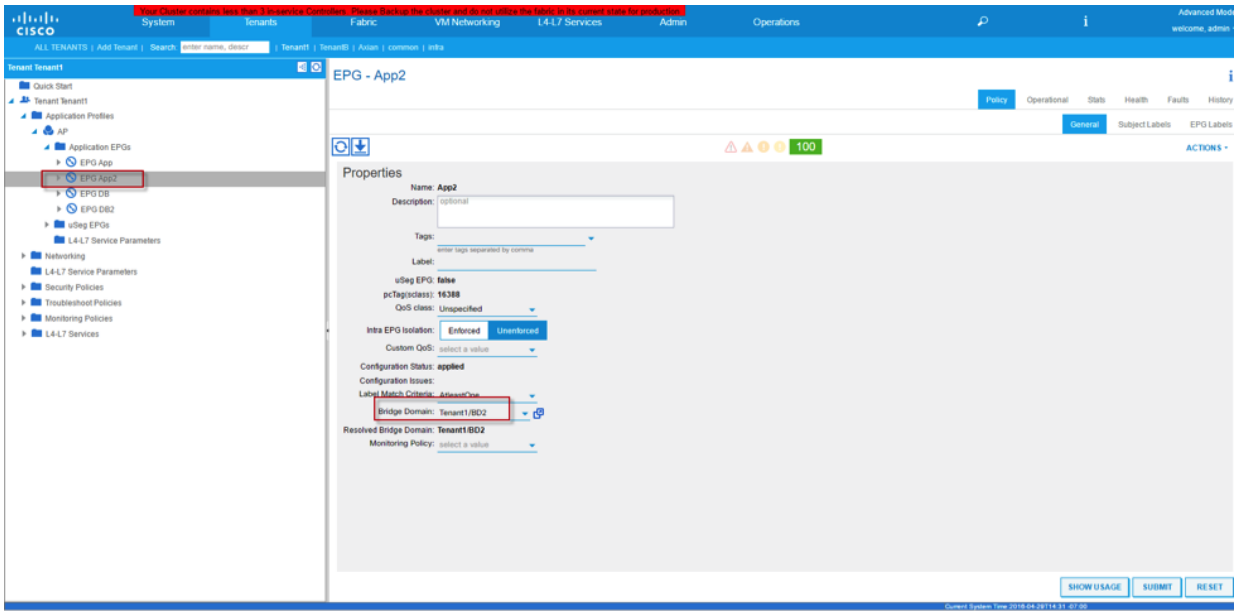


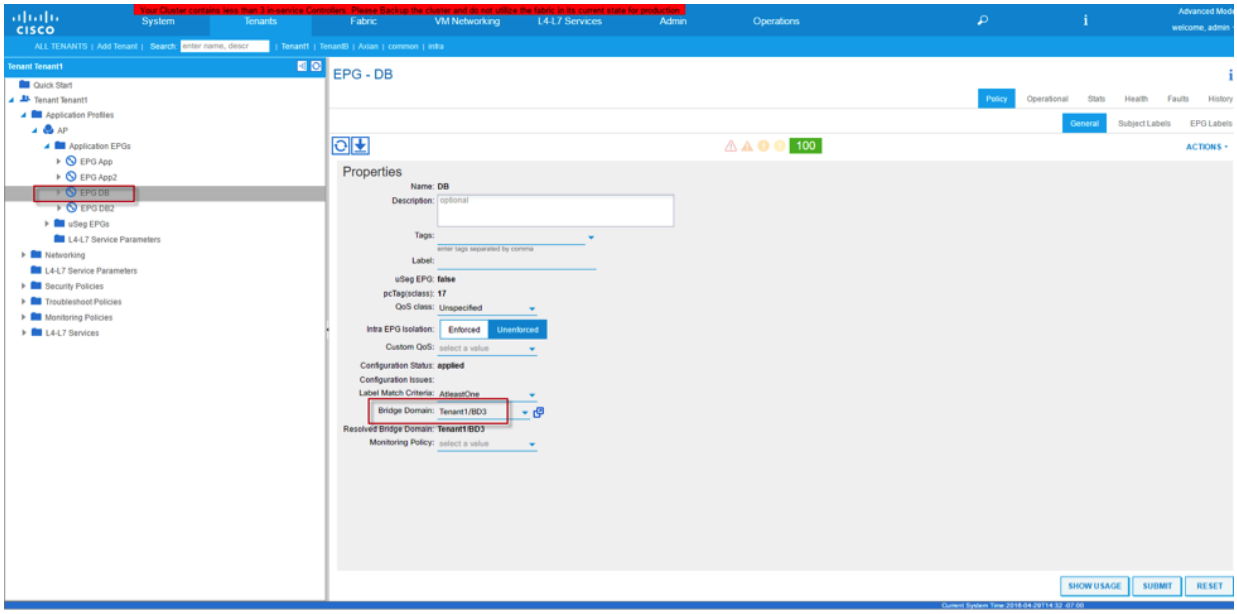
Create 4 EPGs

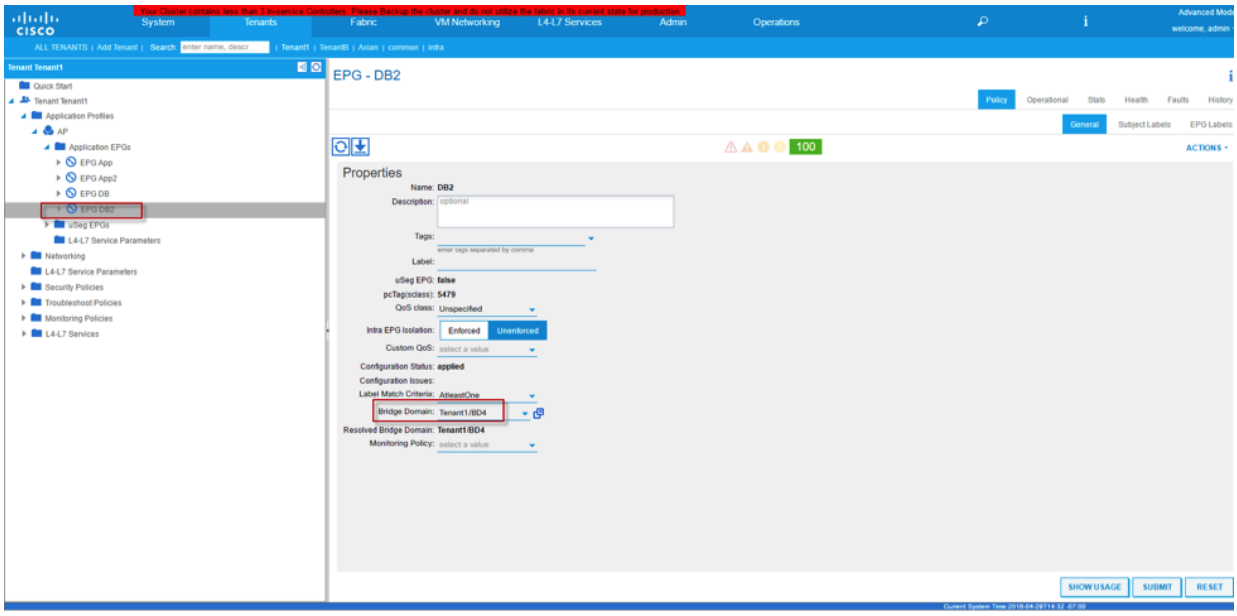


Associate EPG “App”, “App2”, “DB” and “DB2” to Bridge Domain “BD1”, “BD2”, “BD3” and “BD4” respectively

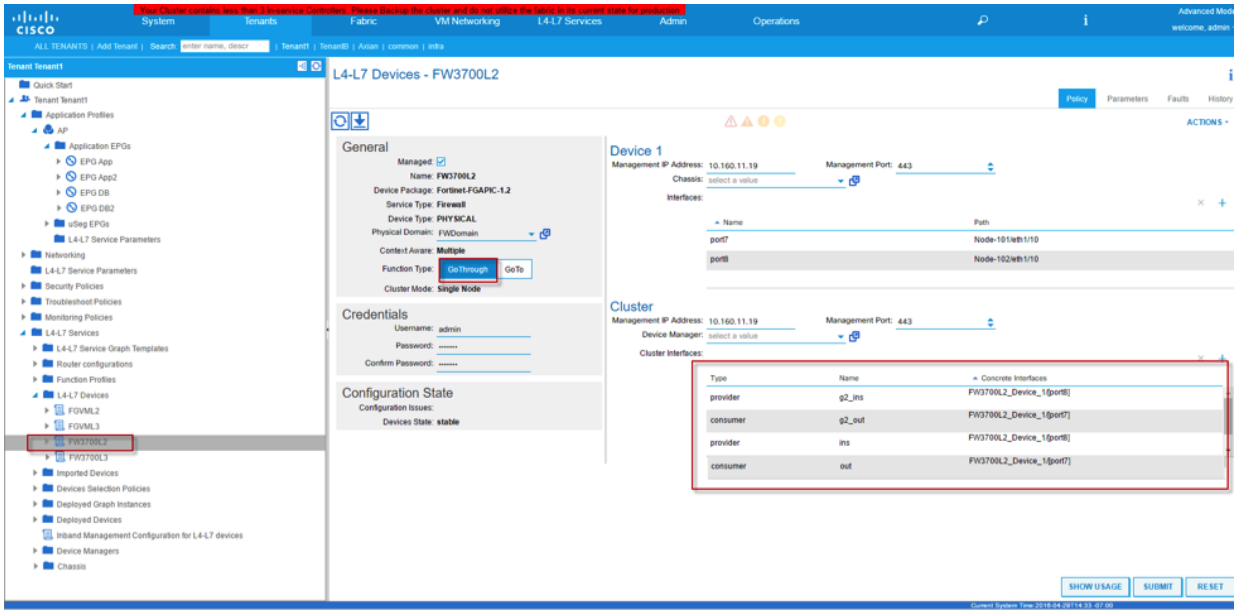



EPG - App2
Properties
Name: App2
Description: optional
Tags:
Label:
uSeg EPG: false
pcTag(sclass): 16388
QoS class: Unspecified
Intra EPG Isolation: Enforced Unenforced
Custom QoS: select a value
Configuration Status: applied
Configuration Issues:
Label Match Criteria: AtleastOne
Bridge Domain: Tenant1/BD2
Resolved Bridge Domain: Tenant1/BD2
Monitoring Policy: select a value
SHOW USAGE
SUBMIT
RESET


EPG - DB
Properties
Name: DB
Description: optional
Tags:
Label:
uSeg EPG: false
pcTag(sclass): 17
QoS class: Unspecified
Intra EPG Isolation: Enforced Unenforced
Custom QoS: select a value
Configuration Status: applied
Configuration Issues:
Label Match Criteria: AtleastOne
Bridge Domain: Tenant1/BD3
Resolved Bridge Domain: Tenant1/BD3
Monitoring Policy: select a value
SHOW USAGE
SUBMIT
RESET

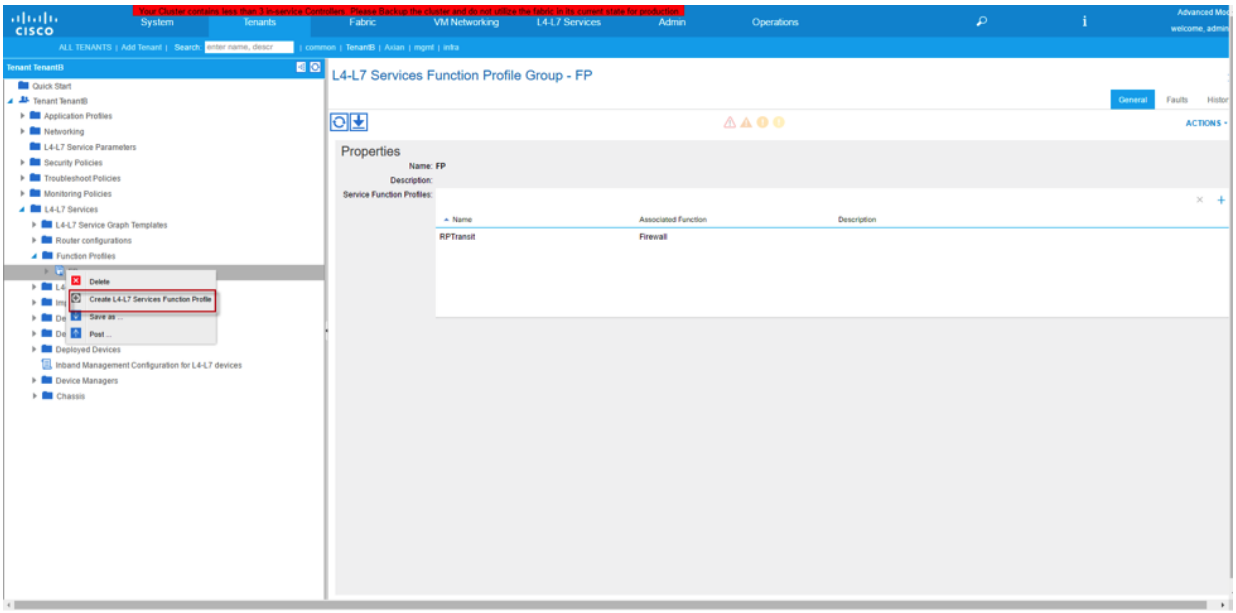


Create Device with Go-Through mode with 4 logical interfaces on Cisco APIC ("Ins" and "Out" for Service Graph 1, "g2_ins" and "g2_out" for Service Graph 2)



Create Functional Profile

Functional Profile defines the template for the Service(s) that is going to deploy such as L4-L7 Device Interface IP addresses, Rule ID, Object Addresses, Policy Rules, Source/Destination Ports…etc.



Functional Profile Objects Explanation under “Features”

Device Network

Contained External and Internal Interfaces that will be programmed onto Fortigate VDOM. This is the interfaces (typically external and internal) that will be associated to the VDOM. Please leave the field in this section untouched for Go-Through mode deployment.

Firewall Objects

This field allows user to customize Firewall Addresses, Service and scheduling.

Firewall Policy Rule

This field encompassed the creation of Firewall policy that will be program onto Fortigate. Security Profile and Logging Options are also configured here.

Static Router

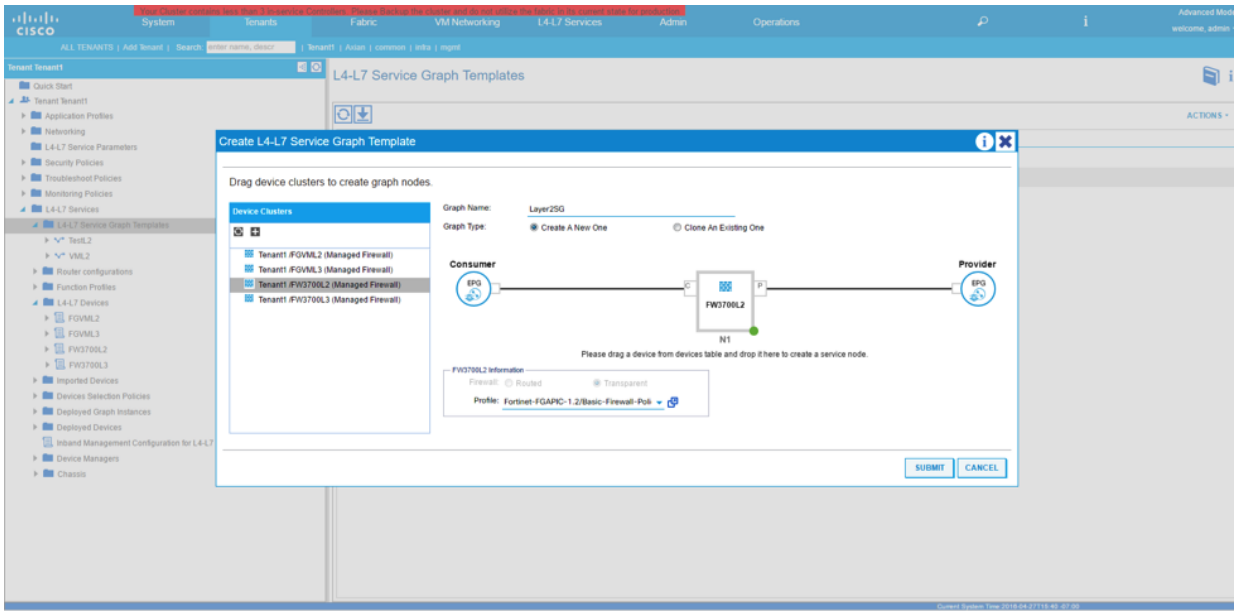
Allow user to configure static route that will be used on Fortigate.

All

This field listed all the parameters stated above plus DDOS configuration.

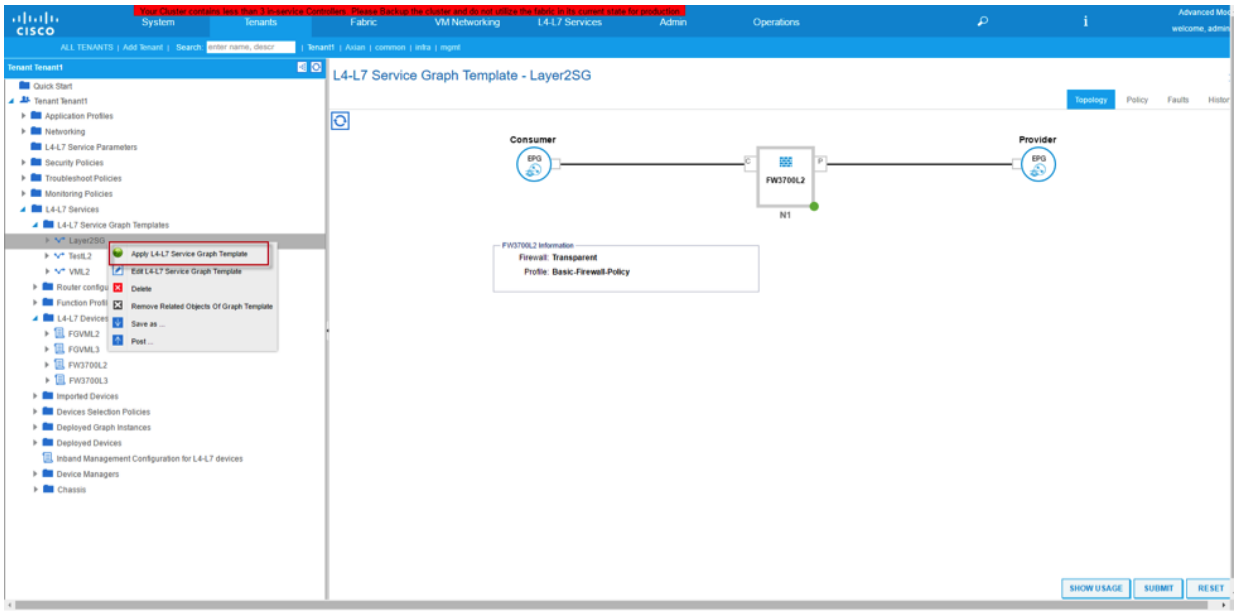
Create Service Graph1

Service Graph template is used to tightly coupled the Functional Profile or Firewall configuration and combine with the Firewall device we defined at earlier steps.

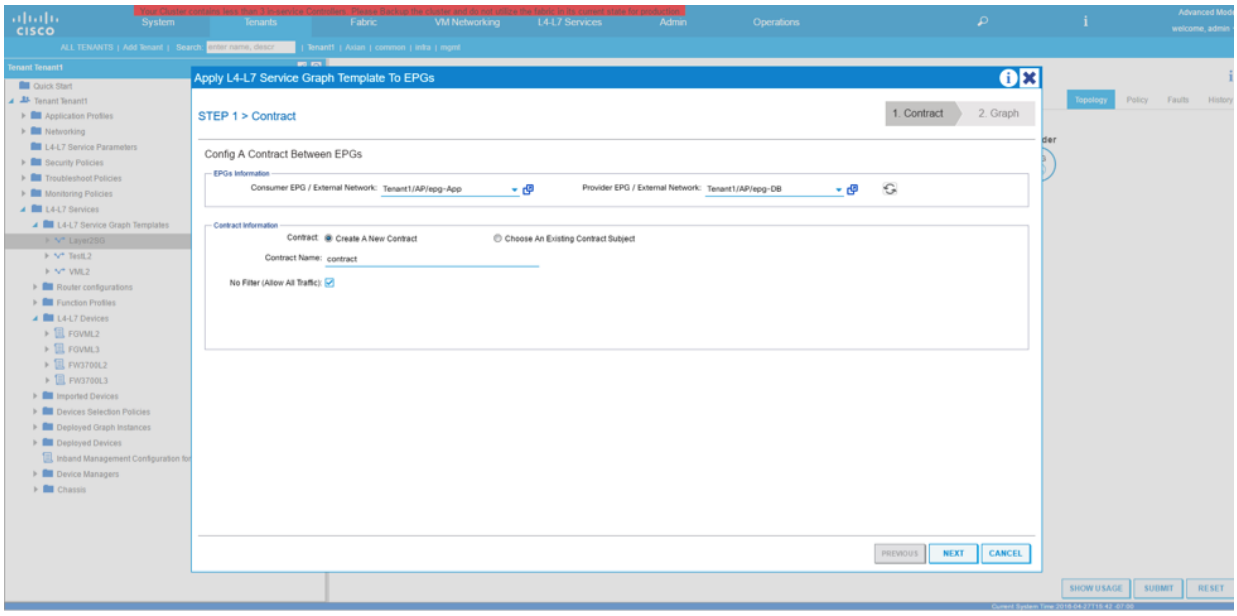


Deploy Service Graph1

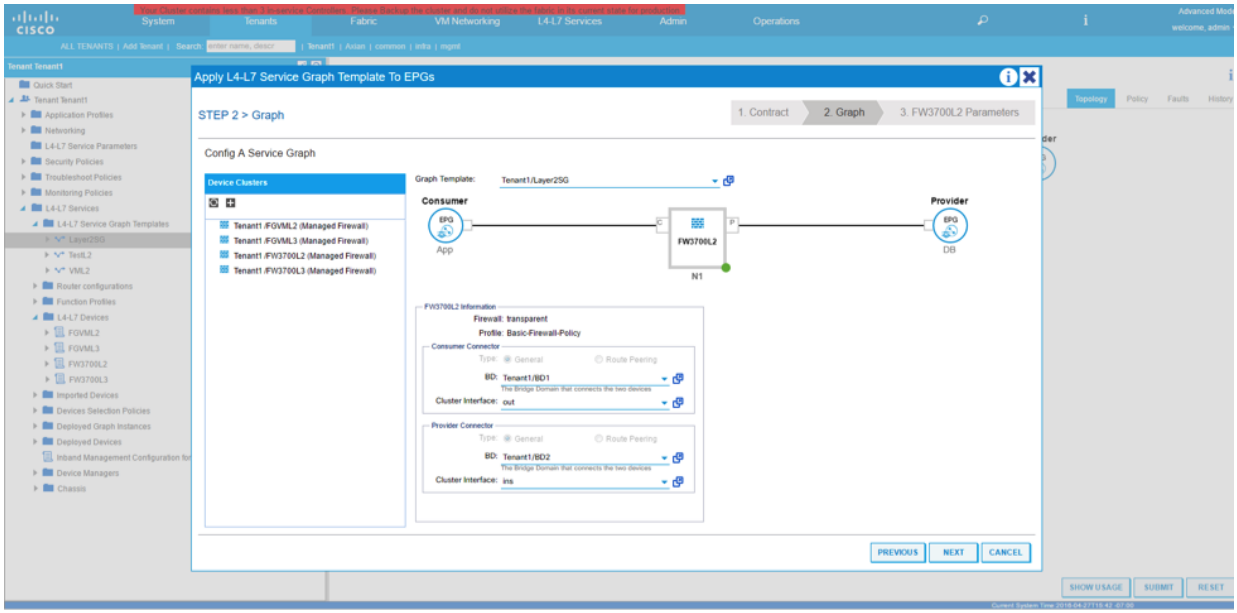
Once we combined the Firewall configuration and associated device together, we are ready to deploy Service Graph 1



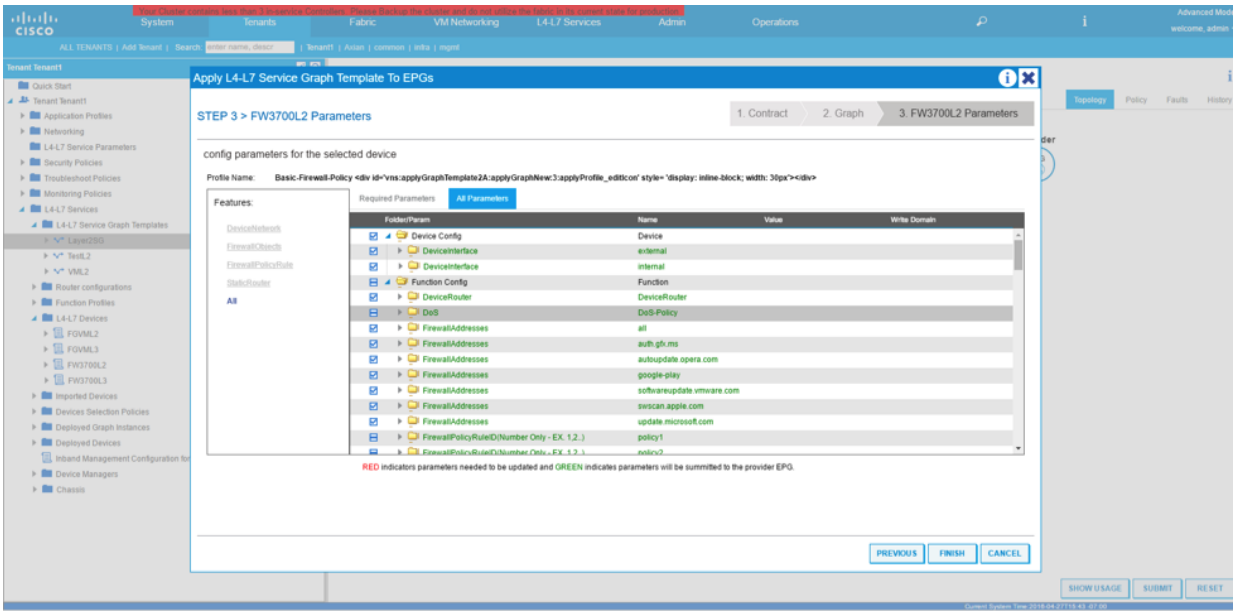
On next screen select the Consumer and provider EPGs (“Apps” and “DB”) and assign a contract name or select a pre-define contract.



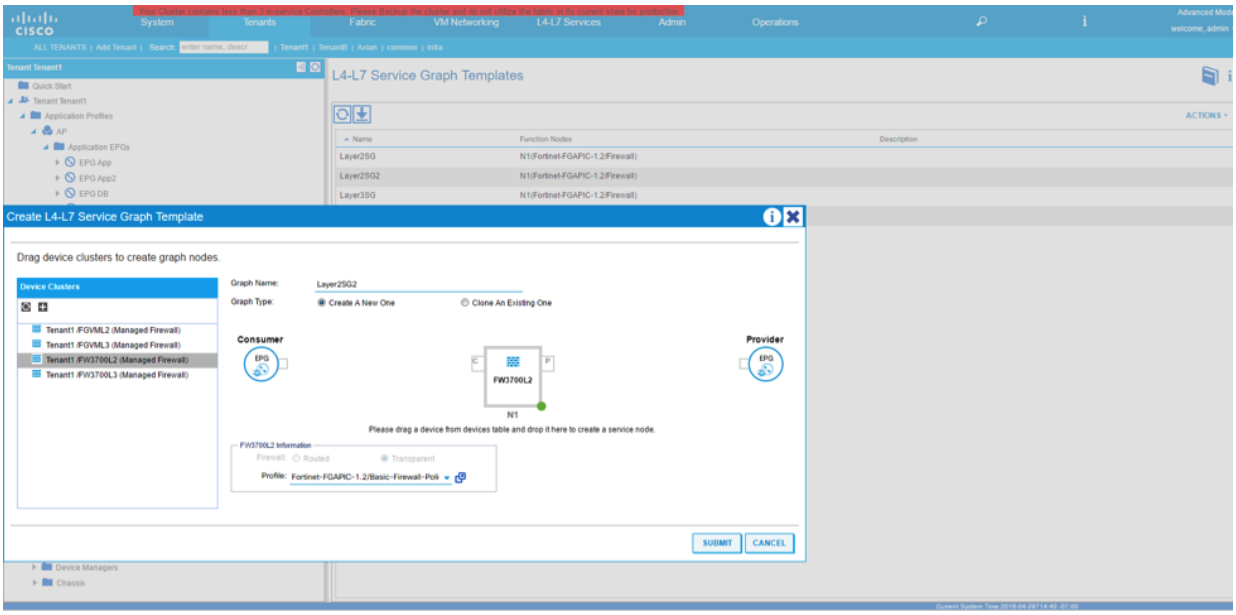
Next screen select the logical interfaces (“ins” and “out”) defined during the creation of Layer4-7 Device.



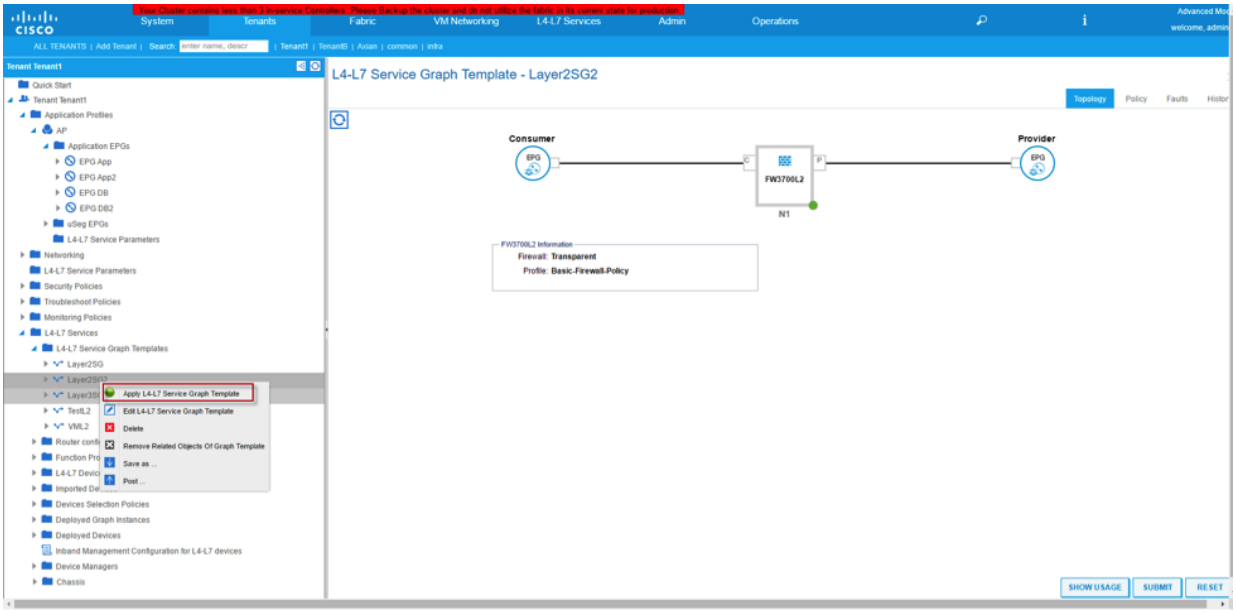
Last minute check to make sure configuration is good before hit “Finish” button



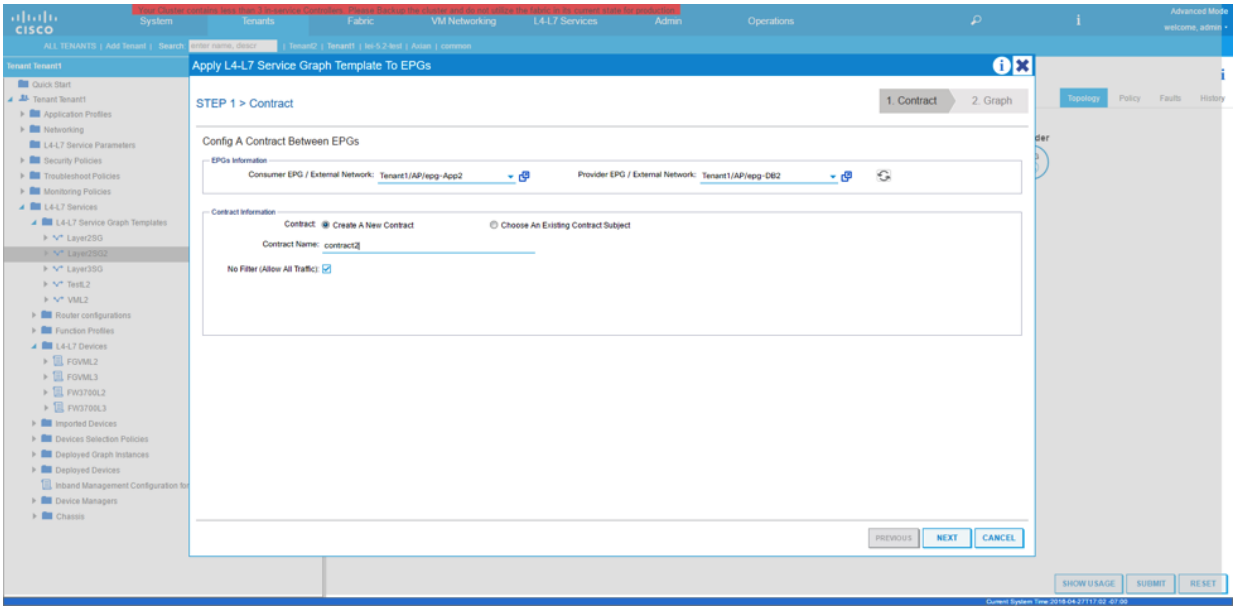
Create Service Graph2



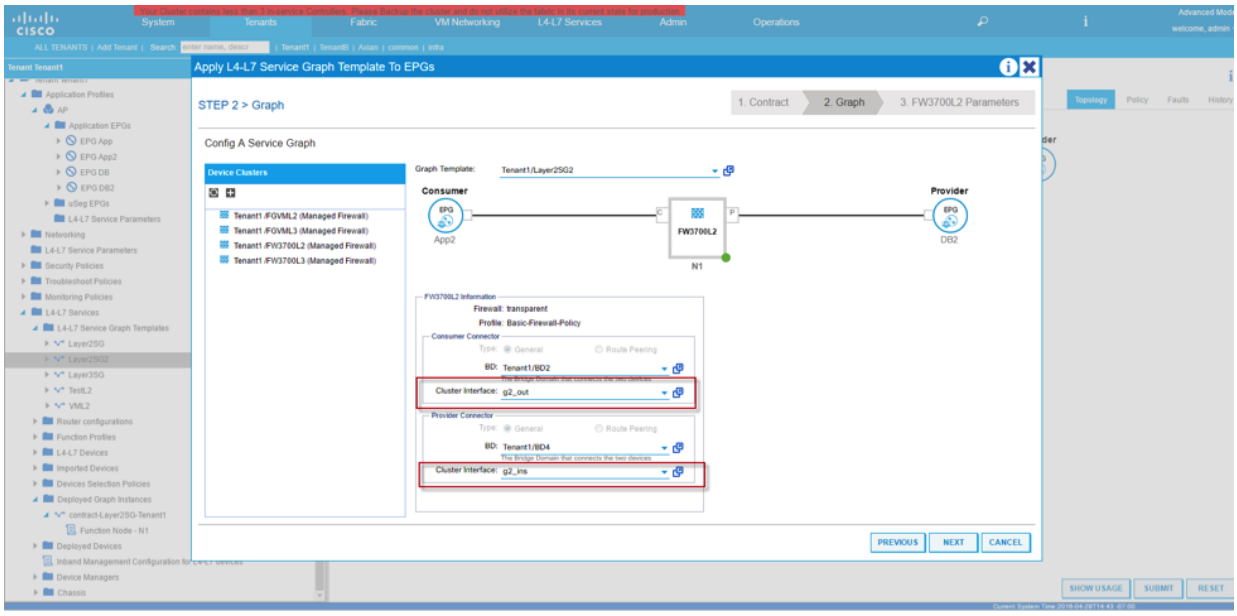
Deploy Service Graph2



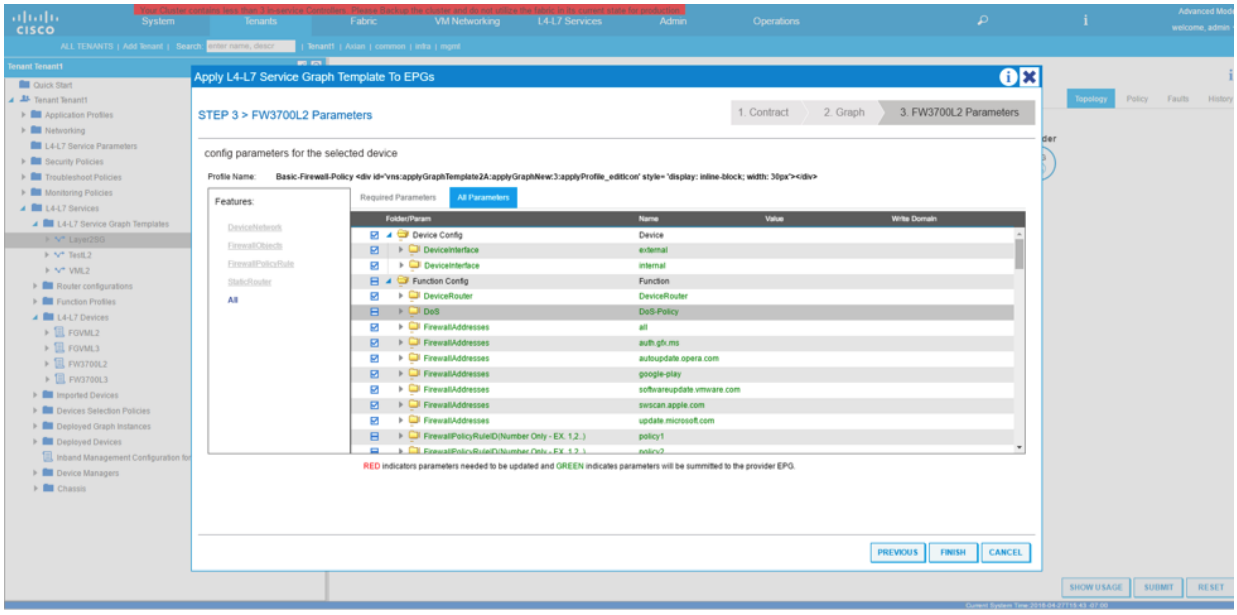
On next screen select the Consumer and provider EPGs (“Apps2” and “DB2”) and assign a contract name or select a pre-define contract.



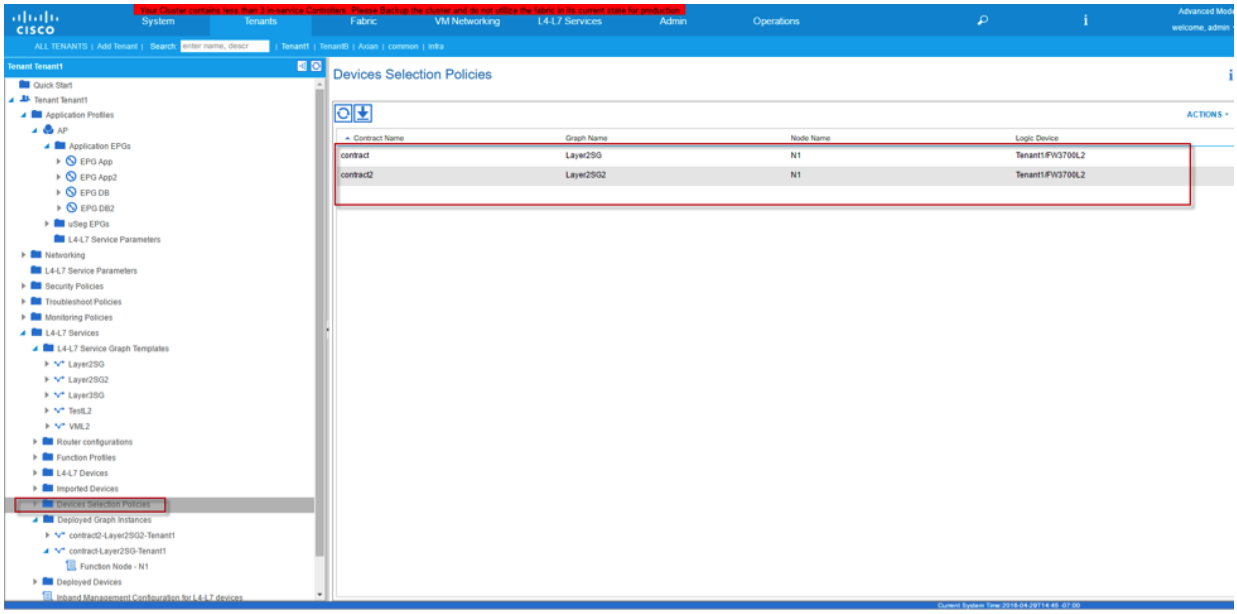
Next screen select the same logical interfaces (g2_ins and g2_out) defined during the creation of Layer 4-7 Device.



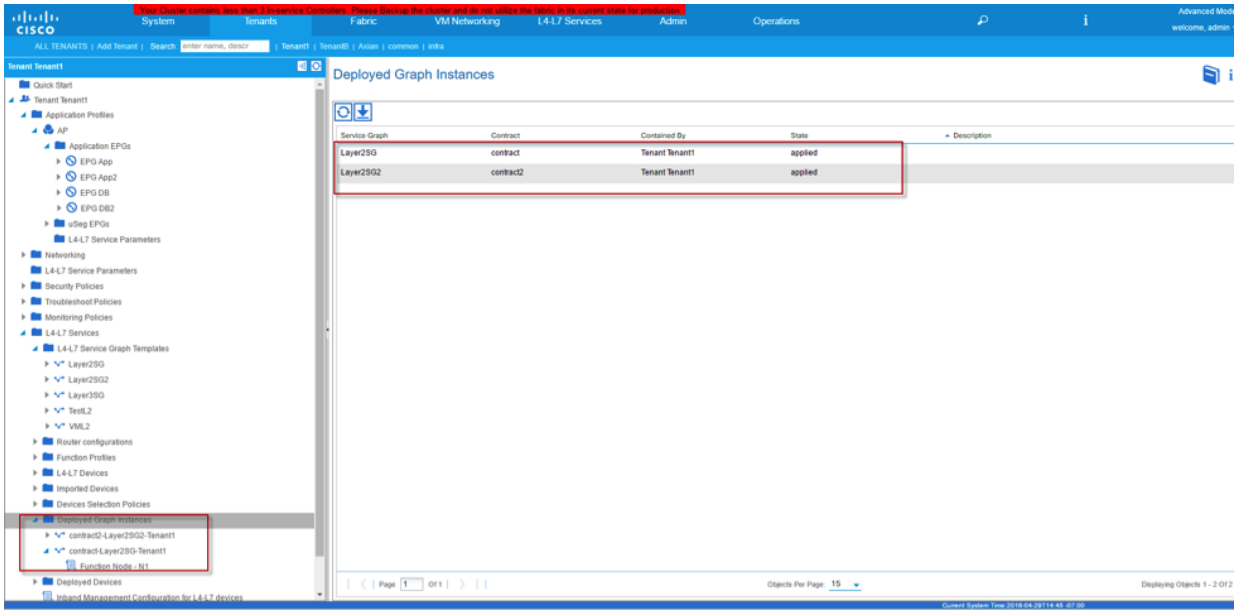
Last minute check to make sure configuration is good before hit “Finish” button

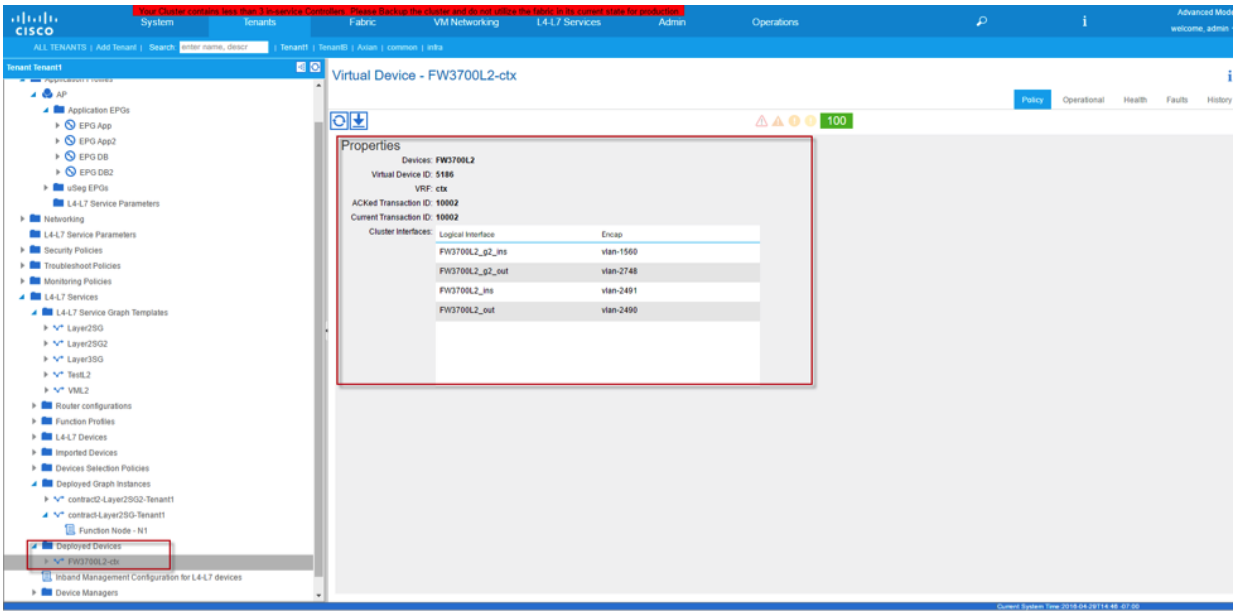


Verify Device Selection Policies Creation



Verify Service Graphs Deployment





Deploying High Availability Service with Cisco ACI and FortiGate

Pre-requisite

On Fortigate:

- Configure Fortigate HA Pair (Active-Standby Mode). Please consult Fortinet support website for setting up HA procedures.

On APIC:

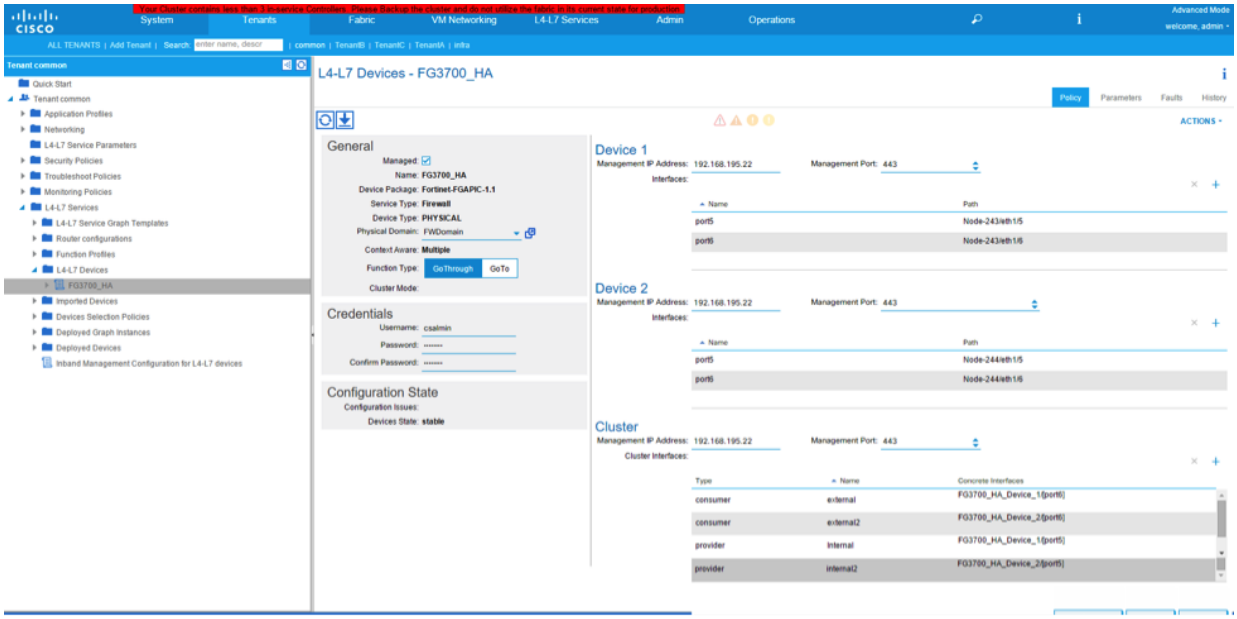
- Fabric Access Policies creation relating to VLAN Pools, Domain, Attachable Access Entity Profiles, Interface Policies and Switch policies.
- Create Tenant, VRF, 2 Bridge Domains, 2 EPGs
- Associate 2 Bridge Domains to VRF
- Associate 2 EPGs to the 2 Bridge Domains
- Layer 4-7 Device Package has imported into Cisco APIC

Work Flow:

1. Create Go-Through Mode with HA enabled, then configure Device #1 and Device #2 on Cisco APIC
2. Create Functional Profile
3. Create Service Graph Template
4. Deploy Service Graph

In general, the procedures to deploy a Go-Through mode HA scenario vs regular Go-Through mode deployment are identical with the exception of enabling HA during L4-L7 device configuration. User needs to select HA Cluster

instead of Single Node for Mode selection; there will be two devices appear on the screen where user will input the same Active Fortigate IP address and the corresponding connection ports between Fortigates and Cisco APIC for both devices. Please see below screen shot for reference.



APIC Infrastructure and FortiGate rollback

1. Upload and unload device package
2. Add and Delete device, FortiGate should clean-up previous configuration.
3. Dynamically modify and update policies
4. Detach and Attach service graphs
5. Delete tenants while service graphs in use.

Basic Troubleshooting

Verify Service Graph deployed

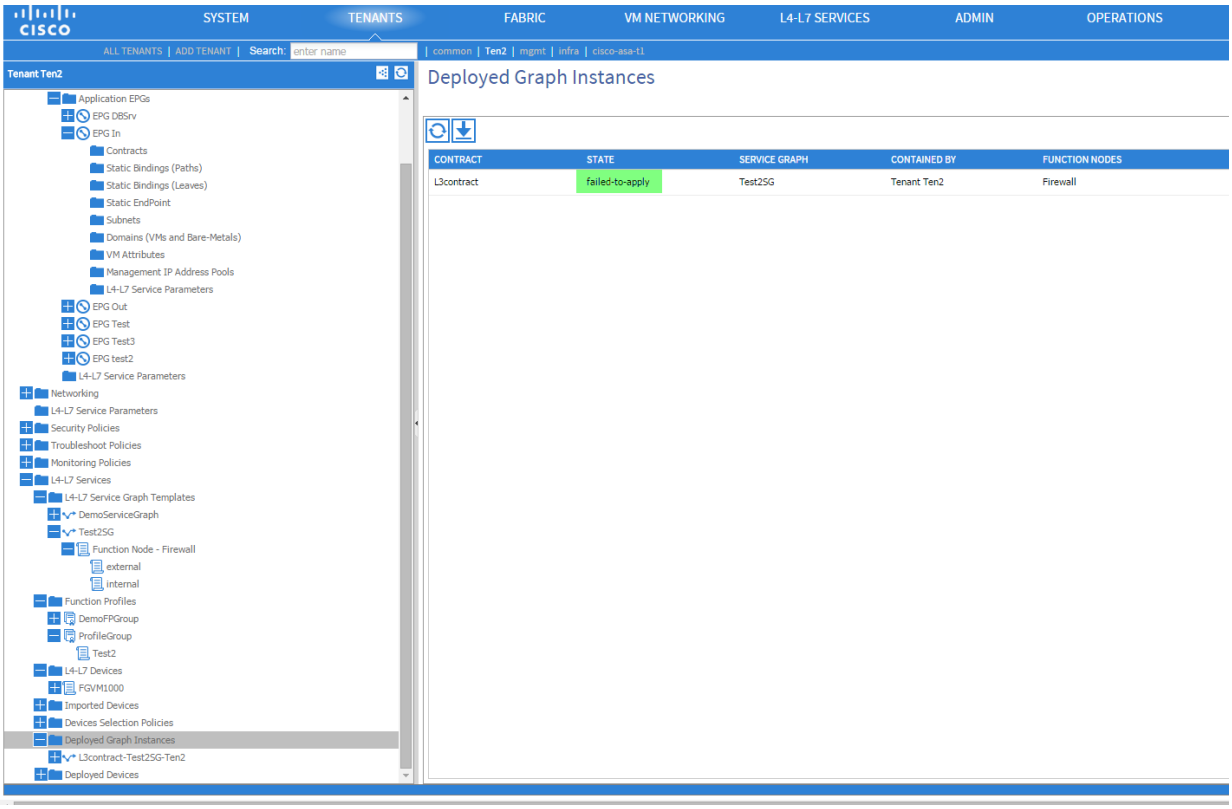
If Service Graph Deployed failed:

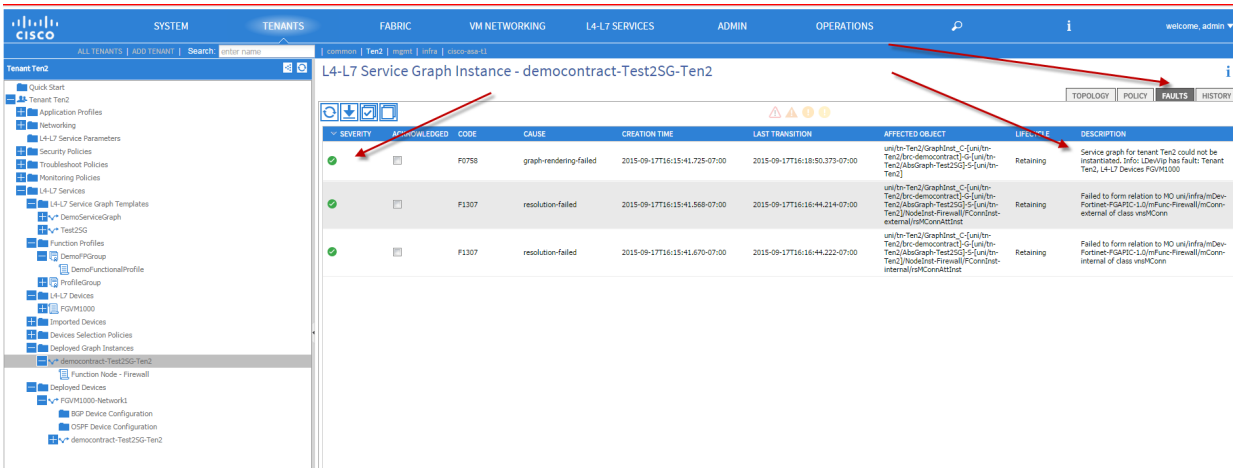
Navigate under ***Tenant > Deployed Graph Instances*** to check the state of the deployed graph.

If state is ***failed apply***, then go down one level to the ***Deployed Graph Instances*** and navigate to the ***Fault*** tab to check the error log. Any error code in 1000 range are relating to FortiGate while others belong to APIC

Currently we only have the following error code:

Error Code	Definition
1010	Configuration Error in device configuration
1020	Configuration Error in function configuration
1030	Internal Error -3
1040	Internal Error -4
1050	Internal Error -5
1070	Feature not available





Service deployed but parameters missing

If Service deployed but certain parameters not showing up on Fortigate, please follow the below steps:

1. Navigate to ***Tenant> Provider EPG>L4-L7 Parameters***, ensure the missing parameters are listed.If not, double check the functional profile to confirm the configuration

FORTINET®

High Performance Network Security